Connecting the Systems that Power Education

Edustructures SIF Agent for SASIxp™

User's Guide
Release 1.1

Edustructures LLC
891 W Baxter Drive
South Jordan, UT 84095
1.877.790.1261

www.edustructures.com

Revision 1.0b – November 2003

Contents

Contents **3**

Part I **6**

Overview **6**

Features 6
Requirements 6
How It Works 7
Where is the Agent Installed? 7
Object ID Database 8
SIF Zones 8
SIF Request & Response 9
SIF Event Reporting 9
SIF Subscription 9
How do I Run the Agent? 10
How do I Configure and Manage the Agent? 10
New Year Rollover Procedure 10

Installation **10**

Java 10
Installer 11
Components 11
The SIF Agent 11
The Object ID Database 11
Centralized Installation 12
Distributed Installation 12
Running the Agent 14
Starting & Stopping the Service 14
Running the Agent as a Standalone Program 14
The Taskbar Icon 15

Part II **16**

Overview **16**

Configuration Overview 16

SASIxp Configuration **17**

Enable Database Monitoring 17
Create the Event Transaction Log (AEVT) 17
Database Configuration 18
dBASE IV ODBC Connection 18
Creating System DSNs for Each School 18
dBASE IV with Qualified Data Files 20
Oracle 20
Microsoft SQL Server 21

Agent Configuration **21**

Settings Dialog Box 21
SASIxp Options 22
Database Type 22
SIF Registration Settings 23
Default SIF Version 24

Agent ID 24
Maximum Buffer Size 24
Messaging Mode 24
Pull Frequency (Seconds) 25
Zone Integration Server — Supported Versions 25
SIF Messaging Settings 25
Request & Response 26
Event Reporting 27
SIF Data Objects Settings 27
Publishing Tab 29
Event Reporting Tab 29
Subscription Tab 30
StudentPersonal Options Tab 30
Field Mappings 31
Field Mapping Rules Summary 32
How to Change Field Mappings for a SIF Data Object 32
How to Customize Field Mappings for a Zone 34
SIF Codes 36
Grade Levels 37
Language 38
Ethnicity 38
English Proficiency 39
StudentContact Type and Relationship 40
Style Settings 41
Telephone 42
Names 42
Addresses 42
Plug-Ins & Macros 43
Reviewing Loaded Plug-Ins & Macros 43
Installing a Plug-In Module 44
Uninstalling a Plug-In Module 45
Transport Settings 46
Protocol 46
HTTP Port 47
HTTPS Port 47
Require Client Authentication 47
Certificate Manager 47
Logging Settings 47
Errors, Warnings, Info and Diagnostics 48
SIF Activity Logging 48
SASIxp Activity Logging 48
Automatic Backup Settings 49

Zone Configuration 50

SIF Zones Overview 50
SASIxp School Zones 50
Aggregate Zones 50
Creating School Zones 50
Creating Aggregate Zones 52
Changing Zone Properties 54
Temporarily Disabling a Zone 55
Deleting Zones 56
Deleting Object IDs 56

Part III 57

The Console 57

Zone Status 57

Activity Tab 59
Pending Events Tab 59
Unreportable Events Tab 60
The Menu Bar 60
File Menu 60
Zone Menu 61
Tools Menu 62

Tools 64

The SASIxp Database Performance Tool 64
Interpreting the Results 65
The SASIxp Event Monitoring Tool 65
Background 66
Using the Tool 66
The Prepare Enrollment Data Tool 67
Object ID Database 69
Backing up the Object ID Database 70
Restoring the Object ID Database from a Backup 71

Part IV 73

Security 73

Authentication 73
Preparing for HTTPS 74
Creating and Importing Certificates for HTTPS 74
Method 1: Creating a Self-Signed Certificate 74
Trusting the Zone Integration Server's Certificate 77
Configuring the Agent & Zones for HTTPS 78
Transport Protocol Settings 78
Zone URL Settings 79

Part V 81

New Year Rollover 81

SIF End-of-Year Procedure 81
New Year Rollover Wizard 82
"It's the end of the current school year" 83
"It's the beginning of the new school year" 83

Part I

OVERVIEW & INSTALLATION

Overview

Features

- SIF 1.1 Compliant. Supports all versions of SIF 1.0r1 and later
- Works in SIF environments where multiple versions of the Schools Interoperability Framework are in use. The agent automatically adjusts the way it performs depending on the version of messages received from the zone integration server.
- Scalable. Supports multiple zones for centralized deployment. The agent can connect to as many zones as necessary from a single server, limited only by available memory, processor speed, and network bandwidth.
- Configurable. Numerous configuration options, including the mapping between SASIxp fields and SIF Data Object fields, can be customized to meet the specific needs of your district. Most aspects of the agent can be configured on a zone-by-zone and SIF version-by-version basis to accommodate the unique integration requirements of each SIF Zone.
- Reliable. The agent can be installed as an NT Service for uninterrupted operation on the Windows NT, 2000, and XP platforms. In addition, it will automatically recover when the connection to the zone integration server or SASIxp database is broken and performs daily automatic backups of its configuration files and Object IDs database.

Requirements

- SASIxp 4.5.2 or later (5.5 or later recommended)
- Supports dBASE IV, Microsoft SQL Server, and Oracle databases
- Microsoft Windows 2000, Windows XP, or Windows 2003. The agent may be hosted on Mac OS X and Linux platforms when used with Microsoft SQL Server or Oracle databases. dBASE IV support is only available on the Windows platform
- Java 1.4 Runtime Environment (J2RE) or later

How It Works

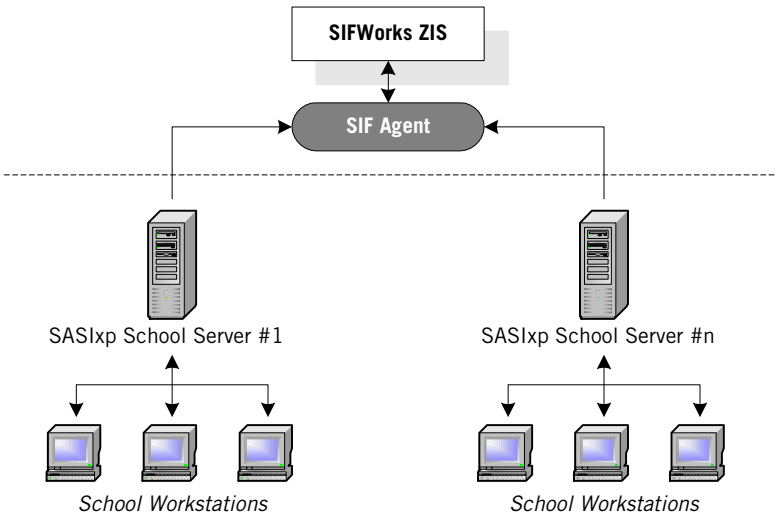
The Edustructures SIF Agent for SASIxp™ is a middleware component that enables real-time data exchange between the SASIxp student management system and applications that support the Schools Interoperability Framework. The agent communicates with the SIFWorks® Zone Integration Server, the central messaging hub in the SIF architecture, to report changes in SASIxp records and to respond to requests for information from SIF-enabled applications.

Where is the Agent Installed?

The SASIxp agent can be installed in both centralized and distributed configurations:

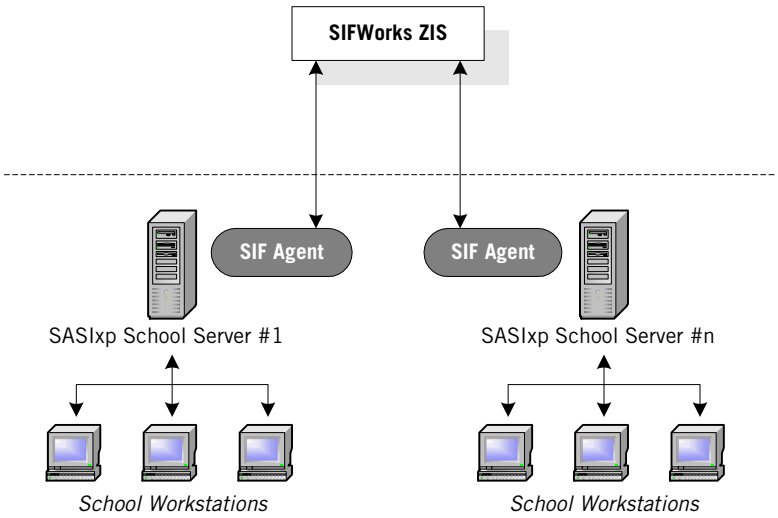
- **Centralized**

  When centralized, the agent is installed on a server at the district office where it can communicate with each SASIxp school server. Centralized installation offers ease of management at the expense of some performance as data must be read from SASIxp databases over the network. (Note the agent does not take part in SASIxp District Integration procedures. Instead, it works with each school on a local basis so data exchange can take place in real-time.)



- **Distributed**

  If network topology or bandwidth limitations prevent the agent from being installed centrally, it can be located on the same server as SASIxp or on another computer at each school. The distributed approach offers the best performance but is more difficult to manage.



Object ID Database

There are two components to the SASIxp agent:

- The SIF Agent software
- The Object ID Database

The Object ID Database is a small relational database that stores the identifiers—also known as *RefIds*—for all SIF Data Objects published by the SASIxp agent. A RefId is a globally unique number that associates a SIF Data Object with its corresponding records in the SASIxp database. RefIds make it possible for all applications that participate in a SIF Zone to refer to objects by a number that is not specific to any one application.

Only one instance of the Object ID Database is required to serve your entire district. When installing multiple instances of the SASIxp agent in a *distributed* fashion, we recommend centralizing the Object ID Database. In other words, install one instance of the database on a central server (e.g. the same computer where the SIFWorks® zone integration server is installed) and multiple instances of the SIF Agent software, one at each school. These will all use the centralized database for Object ID storage. This approach makes it possible to move agents around at a later date without having to merge the Object ID Databases of each school.

After a SASIxp New Year Rollover procedure has been completed, the identifiers in the Object ID Database must be reconciled with student identifiers for the new school year. This mandatory procedure is handled by the agent's New Year Rollover Wizard, described in detail in Part IV of this guide.

SIF Zones

The SASIxp agent is designed around a "one school per zone" model in which each school in your district is represented by a unique SIF Zone. A zone is a logical grouping of data objects and administrative applications that can share objects with one an-

other. The SASIxp agent supports multiple zones, which means it can connect to more than one zone at a time much like an e-mail program can send and receive messages from more than one e-mail server.

Version 1.1 of the SASIxp agent introduces the concept of "aggregate zones". Aggregate zones let you combine one or more school zones into a single zone for easier vertical reporting. For example, you could create an aggregate zone named "DISTRICT" to represent all schools in the district. Agents that request data from this zone would then receive records from all SASIxp schools without having to connect to each school zone individually.

SIF Request & Response

When applications request data from SASIxp through the SIF infrastructure, the agent queries the SASIxp database for records, converts the results to one or more SIF Data Objects, and then returns the results to the zone integration server. The server forwards the responses to each of the requesting applications securely and reliably. You can prevent certain applications from requesting specific types of data by using the Access Control features of the zone integration server.

The following types of records and SIF Data Objects are currently supported:

SASIxp Record Type	SIF Data Object Type
Students	StudentPersonal
Teachers	StaffPersonal
Staff	StaffPersonal
School	SchoolInfo
Basic Student Enrollment	StudentSchoolEnrollment
Parent/Guardian	StudentContact
Rooms	RoomInfo and RoomType

▸ **NOTE:** Refer to the "*Edustructures SIF Agent for SASIxp—Supported SIF Data Objects*" document for a detailed description of the SIF Data objects and elements that are provided by the agent.

SIF Event Reporting

When changes are made to a record in SASIxp, details of the change are recorded in the AEVT Event Transaction Log global data file. The agent periodically reads from this file to report database changes to the zone integration server. When a SIF Event is reported, it is sent to the school zone associated with the data as well as to all aggregate zones of which the school is a member. Event reporting occurs every 60 seconds by default. You can increase or decrease this frequency or turn off Event Reporting altogether from the agent's Settings dialog box.

SIF Subscription

This version of the SASIxp agent is a "read-only" agent, meaning it does not consume SIF Event information reported by other applications. For example, if the name of a student is changed in the library, or the address of a student is updated in the transportation system, those changes will not be propagated to SASIxp.

How do I Run the Agent?

The Edustructures SIF Agent for SASIxp is designed for unattended operation. It is installed as an NT Service on the Windows NT/2000/XP platform. As a service, the agent runs whenever the server is running, regardless of whether or not a user has logged in to that computer. You can stop, start, or restart the service from the Windows Services Manager.

The agent can also be run as a "standalone" application by choosing the "SASIxp Agent - Run Standalone" command from the Edustructures program group on the Windows Start Menu, or by running the SASIxpAgent.cmd batch file from the agent's directory.

▸ **NOTE:** Only one instance of the agent can be running on a given computer. If you start the agent as a standalone application and it is already running as an NT Service, the agent will prevent itself from running a second time.

How do I Configure and Manage the Agent?

The agent features a graphical console from which configuration and management tasks are performed. To display the console window, click the blue and yellow SIF logo on the taskbar near the system clock:

New Year Rollover Procedure

Like SASIxp, the SIF Agent requires that a New Year Rollover procedure be performed in order to reconcile the student identifiers recorded by the agent's Object ID Database with corresponding records in the SASIxp database. This procedure must be started at the end of the current school year **before** performing the SASIxp New Year Rollover, and again at the beginning of the new school year **after** that procedure has been completed.

The agent includes a New Year Rollover Wizard to automate this process, but you must remember to run it before and after the SASIxp rollover procedure. Refer to Part IV of this guide for instructions on New Year Rollover procedures.

Installation

Java

The agent requires that a Java 2 Runtime Environment (JRE) version 1.4 or later be installed. To determine if Java is already installed on your system, open a command prompt and issue this command:

```
java –version
```

If you receive a message that "java" is not recognized as an internal or external command, the Java 2 Runtime Environment is not installed. Visit the Sun website at `http://java.sun.com` to download the latest version.

You can also download a version of the Edustructures SIF Agent for SASIxp installation program that includes a Java virtual machine.

Installer

The installer performs these tasks:

- Optionally installs the Java 1.4 virtual machine
- Copies the program files to your computer
- Optionally installs the "Edustructures SASIxp Agent" Windows Service
- Installs the "Edustructures SASIxp Agent Database" Windows Service
- Creates items on the Windows Start Menu

To run the installer, double-click the `installer.exe` executable and follow the instructions.

Components

There are two components to the Edustructures SIF Agent for SASIxp:

- The SIF Agent
- The Object ID Database

The installation program gives you the choice of installing one or both of these components.

The SIF Agent

The agent is an independent program that can be installed on a central computer or on each computer where SASIxp is installed. By default, it is installed in the `\SIFAgents\Edustructures\SASIxpAgent` directory.

The Object ID Database

The Object ID Database is a small relational database that stores SIF identifiers on behalf of SASIxp. It is installed as a Windows Service and must be running when the agent is running. At least one instance of the Object ID Database must be installed at the district so the agent can keep track of the relationship between records at each school and corresponding SIF Data Objects.

By default, the installer will install both the SIF Agent software and the Object ID Database on the same computer, which is appropriate for centralized installations. For distributed installations, follow the steps in the "Distributed Installation" section below to install a single Object ID Database at the central office, with multiple instances of the SIF Agent software installed at each school.

Centralized Installation

Follow these steps to install the SASIxp agent on a server at the central office:

1. Run the installer.exe executable at a server at the central office

2. When prompted to choose components to install, select "SIF Agent & Database"

3. Follow the steps in Part II of this guide to configure the agent to connect remotely to each SASIxp database instance and school zone

Distributed Installation

Follow these steps to install a single Object ID Database at the central office, with multiple instances of the SIF Agent software installed at each school. The server you choose must have an IP address that can be reached from all other SASIxp school servers on the network. Edustructures recommends using the same server where the SIFWorks® ZIS is installed.

▸ **IMPORTANT:** Distributed installations are rare and applicable only to dBase IV users. If your district uses dBase IV and has a relatively fast network connection between the central office and each school, or if you use Microsoft SQL Server or Oracle, you should probably perform a centralized installation.

1. Run the `installer.exe` executable at a server at the central office

2. When prompted to choose components to install, select "SIF Agent & Database"

Now follow the steps below to install a copy of the SIF Agent (and not the database) at each school. The agent should be installed on a computer that has local access to the SASIxp data file folders.

1. Run the `installer.exe` executable at each school

2. When prompted to choose components to install, select "SIF Agent Only"

3. After the installation is complete, you will need to modify the agent's configuration file to instruct it to connect to the Object ID Database at the central office. Using Notepad or another text editor, open the `agent.cfg` file in the agent's installation directory (e.g. "`\SIFAgents\Edustructures\SASIxpAgent-1.1`").

   Locate the following lines:

```
<database>
   <property name="driver" value="org.hsqldb.jdbcDriver"/>
   <property name="user" value="sa"/>
   <property name="password" value=""/>
</database>
```

   Add a fourth property to this group of settings:

```
<property name="url"
   value="jdbc:hsqldb:hsql://192.168.1.14:16010"/>
```

   Make sure to specify the real IP address of your central server. The address 192.168.1.14 above is an example.

The resulting <database> section should look something like this:

```
<database>
   <property name="driver" value="org.hsqldb.jdbcDriver"/>
   <property name="user" value="sa"/>
   <property name="password" value=""/>
   <property name=”url”
      value=”jdbc:hsqldb:hsql://192.168.1.14:16010”/>
</database>
```

4. Save the file

If the “Edustructures SASIxp Agent” service was started by the installation program, restart it from the Windows Service manager for the new settings to take effect.

Running the Agent

The SASIxp agent is installed as a service on Windows 2000 and XP platforms. When the service is running, the agent will respond to requests from the SIFWorks® zone integration server and continually monitor SASIxp databases for changes made to records. When the agent service is not running—for example, while the computer is starting up or if you have taken the agent down for maintenance—SIF messages will be safely held in the agent’s queue on the zone integration server until the service is again started.

Starting & Stopping the Service

Follow these steps to start and stop the service:

1. Open the Windows Service Manager.

   There are many ways to bring up the Service Manager. On Windows 2000 and XP, the easiest is to right-click My Computer on the desktop, and then choose Manage from the pop-up menu. The Computer Management window appears. Expand the “Services and Applications” node in the tree, and then select the Services entry to view all services on your computer.

2. Highlight “Edustructures SASIxp SIF Agent”

3. Start, Stop, or Restart the service

You will need to return here to restart the service whenever you make changes to the agent configuration.

Running the Agent as a Standalone Program

When the SASIxp agent is run as an NT Service, there is no visible “console” from which to view its activity. Occasionally it is useful to run the agent as a standalone program instead of as a service. This is particularly helpful during initial installation and configuration as well as when trying to isolate a problem.

To run the agent in standalone mode,

1. Make sure the Edustructures SASIxp Agent service is stopped if currently running. You cannot run both the NT Service and the standalone agent at the same time.

2. Choose "SASIxp Agent – Run Standalone" from the **Start Menu > Programs > Edustructures** menu

The agent will run in a Windows command console. To stop the agent, press Ctrl+C or open the agent console window and choose Exit & Shutdown from the File menu.

The Taskbar Icon

When the SASIxp agent is running—either as an NT Service or in Standalone mode—a blue and yellow SIF logo appears on the Windows taskbar near the system clock. Click the icon to open the SASIxp Agent Console.

Note the icon appears gray when the agent is starting up or shutting down. If the icon is missing from the taskbar, it probably means the agent is not running.

Part II

INSTALLATION QUICKSTART

Overview

Agent configuration is an important step in the deployment of SIF Zones. The SASIxp agent is highly customizable, designed to meet the needs of even the most demanding SIF integration project. Configuration choices made for the SASIxp agent depend to a large extent on the requirements and capabilities of other SIF agents in use at the district. You may need to revisit the agent's configuration later on when deploying new agents that subscribe to the SIF Data Objects published by SASIxp.

We divide configuration into two parts: Basic Configuration and Advanced Configuration. Basic configuration involves those steps that are essential to connecting the agent to both the SASIxp™ student information system and the Zone Integration Server. Advanced Configuration involves fine-tuning to address specific integration challenges.

This chapter covers the basic configuration tasks that are mandatory for the successful operation of the agent. Depending on the other SIF-enabled applications at the district, you may need to perform additional customization tasks as discussed in Part III of this guide.

Configuration Overview

Configuration of the SASIxp agent involves the following three tasks, each of which must be performed once for each SIF Zone and SASIxp school the agent will connect to.

- SASIxp Configuration
  - Set options in the `sasixp.ini` file
  - Create the Event Transaction Log
- SASIxp dBase IV Configuration
  - Create an ODBC Data Source for each SASIxp `datafile` directory
- Zone Configuration
  - Add each zone to the agent
  - Adjust global and zone-by-zone settings as needed

SASIxp Configuration

The SIF agent relies on features designed into the SASIxp application to support the Schools Interoperability Framework. In particular, the "database monitoring" feature captures changes made to records in the database so they can be reported as SIF Events by the agent. SIF Events notify other applications of added, changed, and deleted records in real-time. By default, the database monitoring feature is disabled when SASIxp is installed. It must be turned on by following the steps below for each instance of SASIxp.

Repeat the steps below for each school to which the agent will connect.

Enable Database Monitoring

1. Open the **sasixp.ini** file in Notepad. This file is located in the SASIxp directory.

2. Ensure the following 4 lines are present at the end of the file, and that the **UseMonitoring** and **UseEnrMonitoring** entries are set to a value of True. The last entry, **UseAttendMonitoring**, should be set to False in this version of the agent. If the lines are not included in your copy of sasixp.ini, add them to the end of the file exactly as shown below.

```
[Monitoring]
UseMonitoring = True;
UseEnrMonitoring = True;
UseAttendMonitoring = False;
```

SASIxp must be restarted for these changes to take effect.

Create the Event Transaction Log (AEVT)

The Event Transaction Log is a global SASIxp data file that stores a journal of changes made to records subject to database monitoring. Because database monitoring occurs regardless of whether the SIF Agent software is running or not, changes are queued in this file until they can be successfully reported to SIF.

By default, the AEVT file does not exist. Follow the instructions below to create this file in each instance of SASIxp:

1. Login to SASIxp

2. Open the **Create New Files** atom in the **File Management** folder

3. Check the **Use Database Definition** checkbox at the bottom of the Create New Files window

4. Scroll down to the **AEVT – Event Transaction Log** entry. If the "Created" column is empty, click the Create button to create the AEVT file.

Database Configuration

Once you've performed the above steps for each instance of SASIxp, it's time to set up the agent to communicate with the SASIxp database. The agent supports three database configurations:

- dBASE IV
- Oracle
- Microsoft SQL Server

Follow the instructions below for the type of database your district uses.

dBASE IV ODBC Connection

The SASIxp agent uses the Open Database Connectivity (ODBC) standard to read records from dBASE IV data files. ODBC is a technology included with Microsoft Windows and also available free of charge from the Microsoft website. Configuring ODBC for the SASIxp agent involves creating "data sources", or DSNs, that reference files in the datafile folder each instance of SASIxp. The agent uses these DSNs to read records from SASIxp data files.

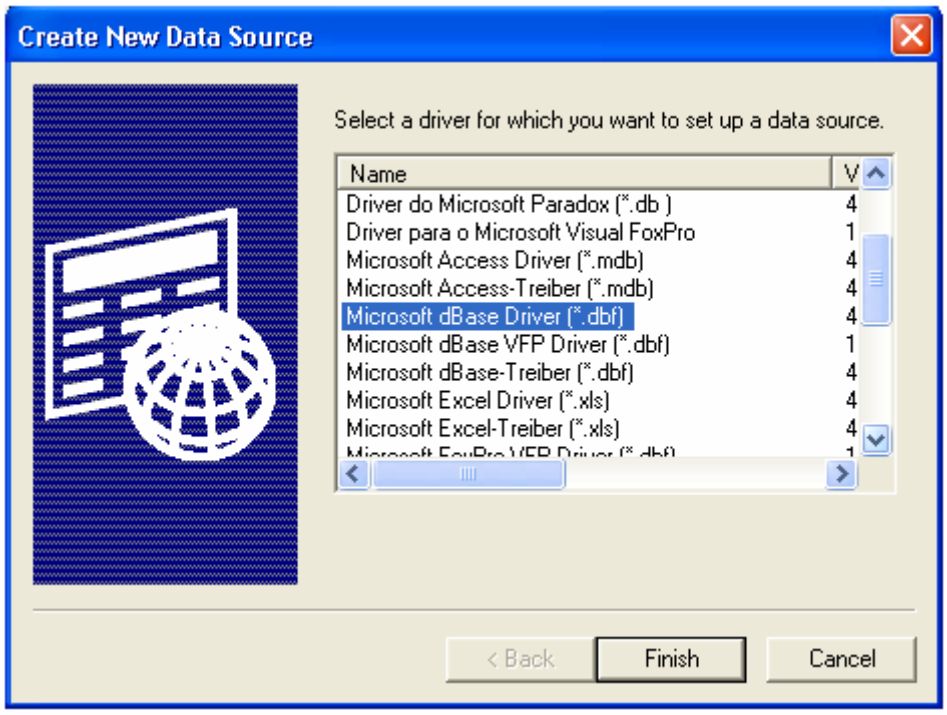
To create and maintain DSNs, launch the Windows ODBC Administrator. You can run this program from the Administrative Tools folder of the Windows Control panel or directly from the agent's Console when creating a new zone.

Creating System DSNs for Each School

You'll need to create one ODBC System DSN for each school to which the agent will connect. In relation to the computer where the SASIxp agent is installed, the schools' data files may be located on a local drive or over the network. When the files are located on a remote computer, use a UNC path instead of a drive mapping to refer to the files (e.g. "`\\JeffersonHS\Vol1\SASIxp\datafiles`").

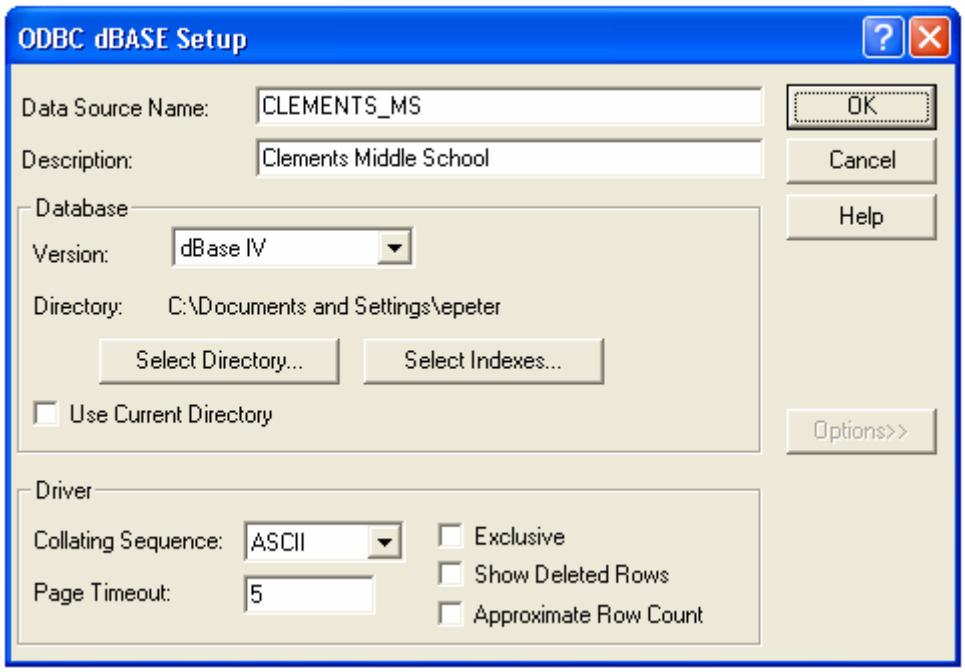
Follow these steps for each SASIxp school the SIF Agent will connect to:

1. From the Windows Start Menu, open the Control Panel
2. Open the **Administrative Tools** Control Panel
3. Choose **Data Source (ODBC)** to launch the ODBC Data Source Administrator
4. Click the second tab, **System DSN**
5. Click the Add… button to add a new System data source:



6. Choose **Microsoft dBase Driver (*.dbf)** from the list

7. Click the Finish button. The ODBC dBASE Setup dialog box appears:



8. Enter a Data Source Name of your choosing.

   For consistency, we recommend using the SIF Zone ID as the Data Source Name (e.g. "CLEMENTS_MS" for Clements Middle School). You may choose any name as long as it is unique and does not conflict with another System DSN entry that has already been created.

   Also enter a description such as "Clements Middle School".

9. Choose "dBase IV" from the Database drop-down list.

10. Uncheck the "Use Current Directory" checkbox, then click the Select Directory button and browse to a SASIxp datafile directory where the school's data files are located. You should use a UNC path instead of a mapped network drive if the SASIxp datafile directory is on another computer. UNC paths are in the form "`\\server\share\path`". Once you've selected the datafile directory, the OK button will become available. Click it to save your selection and close the dialog box.

11. Click the "Options" button to display additional Driver options. Ensure the "Show Deleted Rows" checkbox is cleared. All other settings should be left at their default values.

    ▸ **IMPORTANT:** The Show Deleted Rows checkbox **must not** be checked or the SIF Agent will not function properly.

12. Click the OK button to save your new System DSN

Repeat steps 4-12 to create a System DSN for each SASIxp school.

dBASE IV with Qualified Data Files

If your district uses the "Qualified Data Files" option of SASIxp—that is, each school's data files for each year are located in an independent sub-directory of the root *datafiles* folder—additional steps are required. First, follow the instructions in the previous section to create a System DSN for the school's datafiles folder. Next, create an additional System DSN entry that refers to the root datafiles directory where the global SASIxp files, such as AEVT, are located. This second DSN is needed because the AEVT file is located in a different physical directory that each school's qualified data files.

Oracle

The agent connects to Oracle databases directly without the need for an ODBC driver. To configure the agent to connect to your Oracle server, please gather the following information before proceeding to the chapter on Agent Configuration:

- The IP address of the Oracle server
- A username and password with permissions to access the SASI database

Microsoft SQL Server

The agent connects to Microsoft SQL Server databases directly without the need for an ODBC driver. To configure the agent to connect to SQL Server, please gather the following information before proceeding to the chapter on Agent Configuration.

- The IP address of the SQL Server
- A username and password with permissions to access the SASI database
- If the owner of SASIxp tables is different than the username used to login to SQL Server, you must type the owner name into the SASIxp agent. When the agent queries records from SQL Server, it will prefix each table name with this owner name.

Agent Configuration

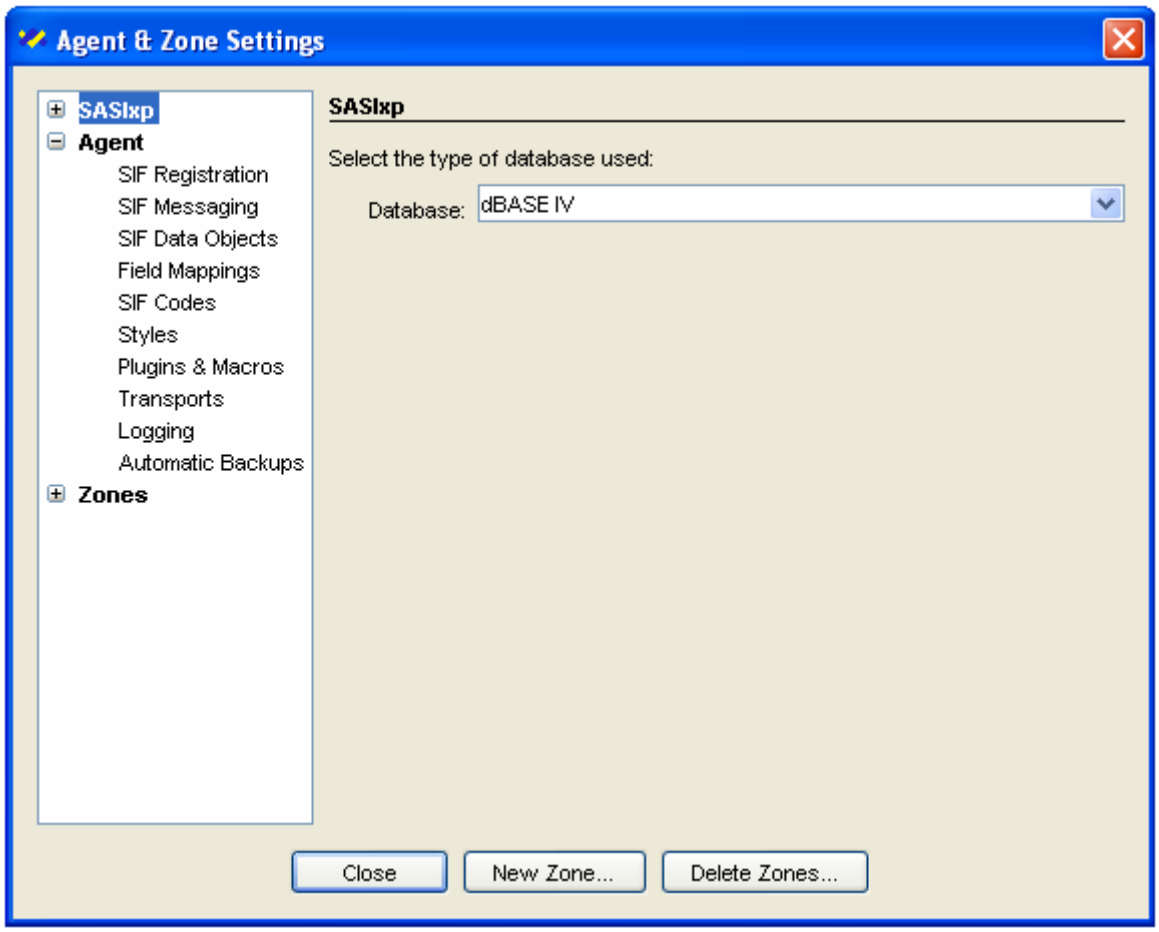
Once each instance of SASIxp has been configured as outlined in the previous section, you're ready to configure the settings of the agent. The agent's factory default settings are appropriate for most installations.

Settings Dialog Box

All agent and zone settings are configured from the Console's **Agent & Zone Settings** dialog box. To open this dialog box,

1. Start the agent if not already running
2. Click on the SIF logo on the system tray to open the Console
3. Choose **Settings** from the Tools menu

The Agent & Zone Settings dialog box opens:



Settings are arranged in a tree shown to the left of the dialog box. To edit a group of settings, click a node in the tree.

SASIxp Options

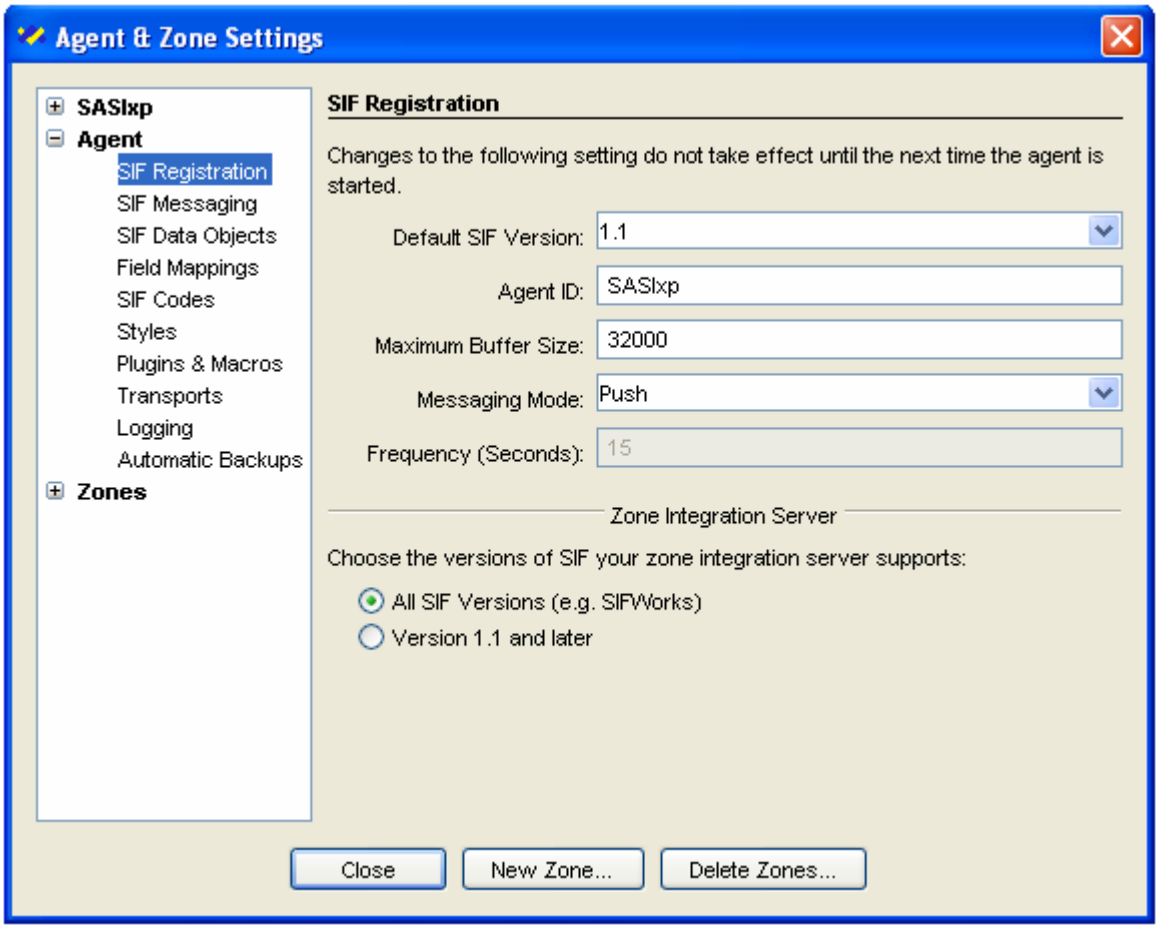
Database Type

The **SASIxp** group of settings applies to all zones to which the agent connects. Here you can choose the type of database your district uses: dBASE IV, Oracle, or SQL Server. Note you must choose a value for this setting before creating new zones.

1. Click the **SASIxp** node in the tree
2. Choose the database type from the drop-down list
3. If you're using dBASE IV, no additional database settings are required.
4. If you're using Oracle or SQL Server, fill in the database connection parameters

SIF Registration Settings

SIF Registration settings control how the agent registers with zones managed by the SIFWorks® zone integration server. The factory defaults are recommended for most installations.



In order to send and receive messages from a SIF Zone, the Schools Interoperability Framework requires that each agent "register" with the zone. During registration, the agent sends a series of commands to the server informing it of various operational settings such as the name of the agent, whether it will use Push or Pull mode to retrieve messages waiting in its queue, the maximum size of messages the agent can receive, the SIF Data Objects the agent provides and subscribes to, and so on. Once registered, an agent remains in this state until it sends the server a command to unregister or until manually deregistered by the ZIS administrator.

The SASIxp agent performs the registration process automatically at startup. If it cannot connect to a zone because of an error or because the zone integration server is offline, it will periodically retry until a connection is established.

Default SIF Version

This setting specifies the version of the SIF specification that the agent uses to report SIF Events to zones. Although the SASIxp agent can receive and process messages in any version of SIF—including 1.0r1, 1.0r2, and 1.1—it will only report SIF Events using the version of the specification chosen here.

Factory Default
The factory default is SIF 1.1

When to Change
Administrators must choose the version of SIF the agent will use to report SIF Events. Select the version that is used by the majority of your subscribing agents. SIF 1.1 specifications dictate that a given message can only be delivered to those agents that support the version of SIF used to produce the message. Consequently, if a subscribing agent does not support the version of SIF selected here, it will not receive SIF Events from SASIxp (messages destined to this agent would be discarded by the zone integration server).

Agent ID

This setting specifies the name the SASIxp agent is known by in the zone. With the SIFWorks zone integration server, you must first add the SASIxp agent to each zone using this name before the agent will successfully connect. The default is "SASIxp", which is case-sensitive.

Factory Default
The factory default is "SASIxp"

When to Change
Administrators rarely if ever change this setting. If changed, the agent must be restarted and re-registered in each zone.

Maximum Buffer Size

This setting specifies the maximum size of messages that can be received by the SASIxp agent.

Factory Default
The factory default is 32,000 bytes

When to Change
Administrators rarely change this setting

Messaging Mode

This setting determines whether the agent will use Push or Pull mode to retrieve messages waiting in its queue on the zone integration server. "Push" mode means the server will send messages to the agent as soon as they become available in the agent's queue. This mode requires that the server be able to communicate with the agent's IP address and port.

In cases where a firewall sits between the agent and ZIS, or when the agent is running on a non-routable IP address that cannot be contacted by the ZIS, "Pull" mode can be used. Pull mode is much less efficient than Push mode because the agent must periodically send commands to the server to check for new messages in its queue. However, Pull mode makes it possible for the agent to exchange messages with the server even if the server cannot "see" the agent because of network or firewall configuration issues.

Factory Default
The factory default is Push mode

When to Change
This setting is usually selected at installation time and not changed thereafter. Changing the messaging mode requires the agent be restarted. If one instance of the agent is connected to many zones (e.g. over 25), Pull mode is not recommended because the agent will spend much of its free time checking for new messages. If you are connecting a single instance of the agent to many zones and must use Pull mode, make sure to expand the Pull Frequency to the 5-15 minute range. This will give the agent ample time to send its Pull requests to each zone before repeating the process.

Pull Frequency (Seconds)

This setting is valid only when Messaging Mode is set to "Pull". It defines the number of seconds between Pull requests. A lower value will cause the agent to spend more time checking for messages, while a higher value (e.g. 10 minutes or 600 seconds) will still achieve the near "real-time" interoperability SIF is famous for while greatly reducing network and processing overhead.

Factory Default
The factory default is 30 seconds

When to Change
Optionally change this setting when changing the Messaging Mode to "Pull", or if you determine a faster or slower polling frequency is warranted.

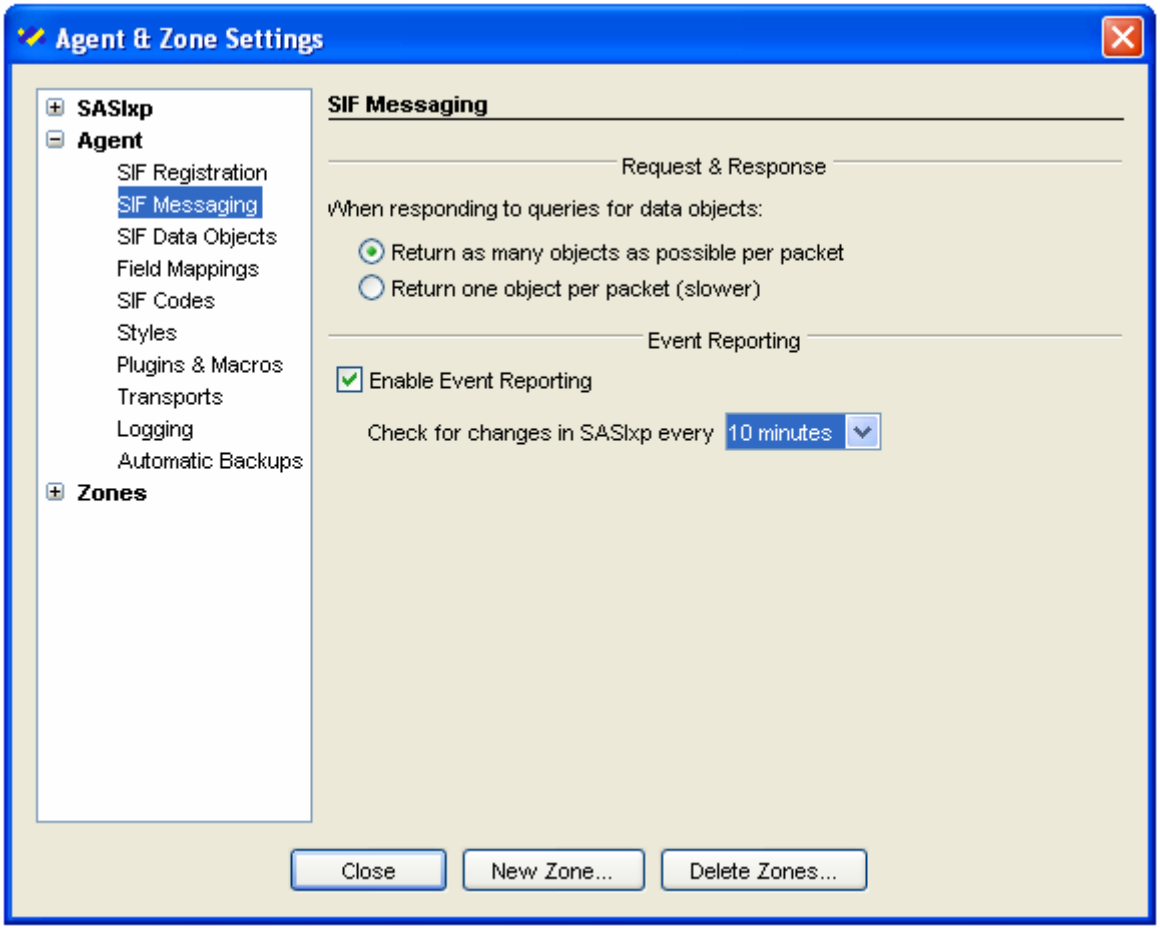
Zone Integration Server — Supported Versions

This group of settings controls how the agent registers with the zone integration server. Some ZIS products on the market do not allow agents to register in support of SIF versions older than 1.1. If connecting to a zone integration server that enforces this restriction, choose the "Version 1.1 and later" radio button. If connecting to the Edustructures SIFWorks® Enterprise ZIS, which supports all versions of the Schools Interoperability Framework, choose the "All SIF Versions" radio button. This is the factory default.

SIF Messaging Settings

SIF Messaging settings control how the agent sends responses to queries and how often it checks SASIxp for changes in record data. The factory defaults are recom-

mended for most installations, although you may wish to decrease the Event Reporting frequency to reduce network traffic and access to the SASIxp database files.



Request & Response

This group of settings controls how the agent sends responses to queries. If the "Return as many objects as possible per packet" radio button is selected, the SASIxp agent will fit as many objects into each response message as possible. The requesting agent's maximum buffer size is used to calculate the size of response packets. For example, if a requesting agent with a maximum buffer size of 100K bytes queries SASIxp for all student records, the agent will divide the responses into chunks of 100K, perhaps resulting in a few dozen messages depending on the number of students in the school. This approach results in the optimal number of packets, thereby reducing network and processing overhead.

In some cases, particularly during diagnostics, it may be desirable to have the agent respond to queries with a single packet per object. To enable this mode, select the "Return one object per packet (slower)" radio button. For example, if a requesting agent issued a query for all students and 1200 students were enrolled in the school, the SASIxp agent would respond with 1200 individual packets, each consisting of one

student object. This mode results in much slower overall processing by the requesting agent because it must process many more messages.

Factory Default
The factory default is "Return as many objects as possible per packet"

When to Change
Change this setting to "Return one object per packet" only when it is easier to diagnose problems if query responses are packaged into individual response packets (e.g. one record in a response is resulting in an XML Validation error but you're not sure which one). Once you've isolated the problem, revert to the "Return as many objects as possible per packet" setting.

Event Reporting

This group of settings controls how the agent reports SIF Events when changes are detected in the SASIxp database.

Use the "Enable Event Reporting" checkbox to enable or disable event reporting. When disabled, the agent does not periodically check the SASIxp Event Transaction Log file (AEVT) for changes. Any changes made in SASIxp's database will be queued in this file until event reporting is enabled again.

When Event Reporting is enabled, the agent polls the AEVT file at regular intervals. The "Check for changes in SASIxp every N seconds" setting specifies the polling frequency. A lower number will result in slower performance because the agent reads from the SASIxp database more often. However, changes made in SASIxp will appear in subscribing agents more quickly. A larger value, such as 10 minutes, is recommended because the agent will spend less time checking for changes yet they're still reported to subscribing applications in relatively quickly—at most 10 minutes after the change is made in SASIxp.

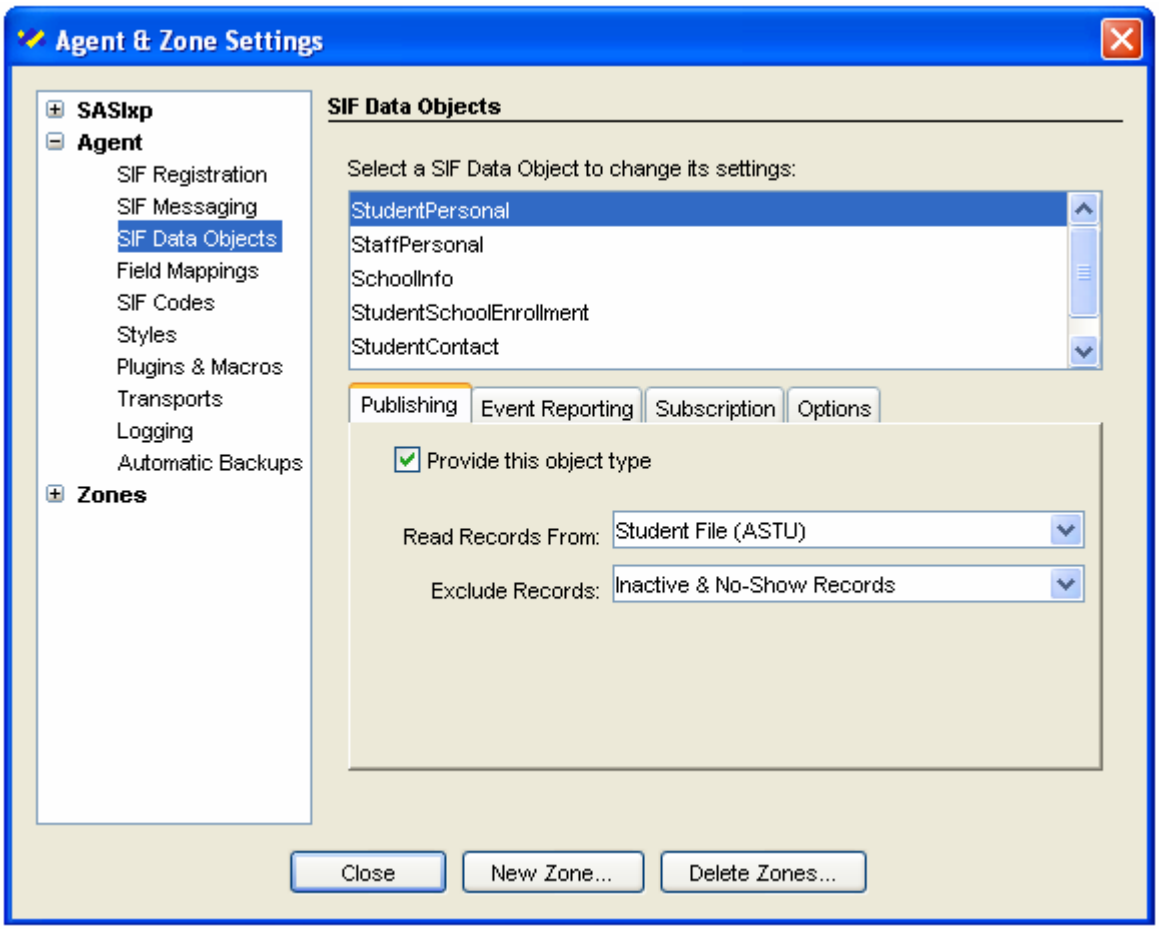
As with all time-based settings, lower values are usually selected when diagnosing problems or learning the system. For example, when testing that Event Reporting is working properly, it is tedious to wait 10 minutes for a sample change in SASIxp to be reported. A much smaller setting of 15 seconds, while unnecessary for a production environment, is easier to work with during testing.

Factory Default
The factory default is 30 seconds

When to Change
Decrease the polling frequency by setting this value to a larger number such as 10 minutes after you've installed the SASIxp agent and have successfully tested that event reporting is working as expected.

SIF Data Objects Settings

This group of settings controls how the agent publishes and reports events for the SIF Data Objects supported by the agent.



To change the properties of a SIF Data Object, select it in the list. Most objects offer three of four tabs depending on its capabilities:

- **Publishing.** These options determine whether the SASIxp agent registers in SIF Zones as the authoritative provider of this type of object. For most object types you can configure additional settings that control how records from SASIxp are published to SIF.

- **Event Reporting.** These options determine the kinds of actions in SASIxp that will result in SIF Events reported to zones. For most object types you can enable or disable the reporting of added, changed, and deleted records.

- **Subscription.** These options determine whether the SASIxp registers as a Subscriber of this object type in SIF Zones (not supported in this release.)

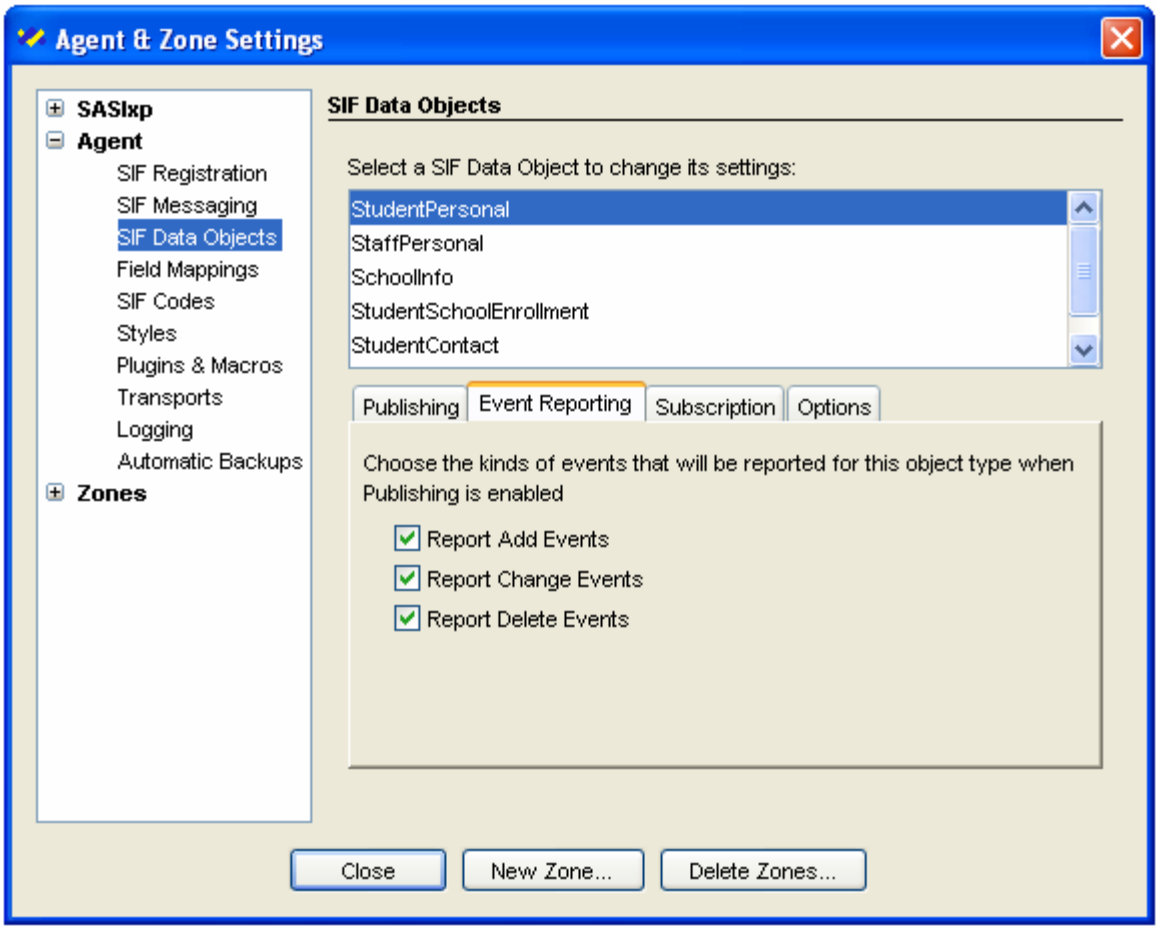
- **Options.** If additional configuration options are available, an Options tab is displayed. For example, when choosing the StudentPersonal object type you can enable dynamic address completion for empty addresses.

Publishing Tab

Check the "Provide this object type" checkbox to register as the authoritative provider of the selected SIF Data Object in each zone. While most districts will want to enable this checkbox, there are cases when another SIF Agent should be the provider of an object type. For example, you may have a third-party attendance package that is considered to be the authoritative provider of all student attendance data. In this case, use the Publishing tab to disable the SASIxp agent's attendance objects.

Event Reporting Tab

Check the types of SIF Events that should be reported by the agent. In general, these checkboxes should always be enabled.



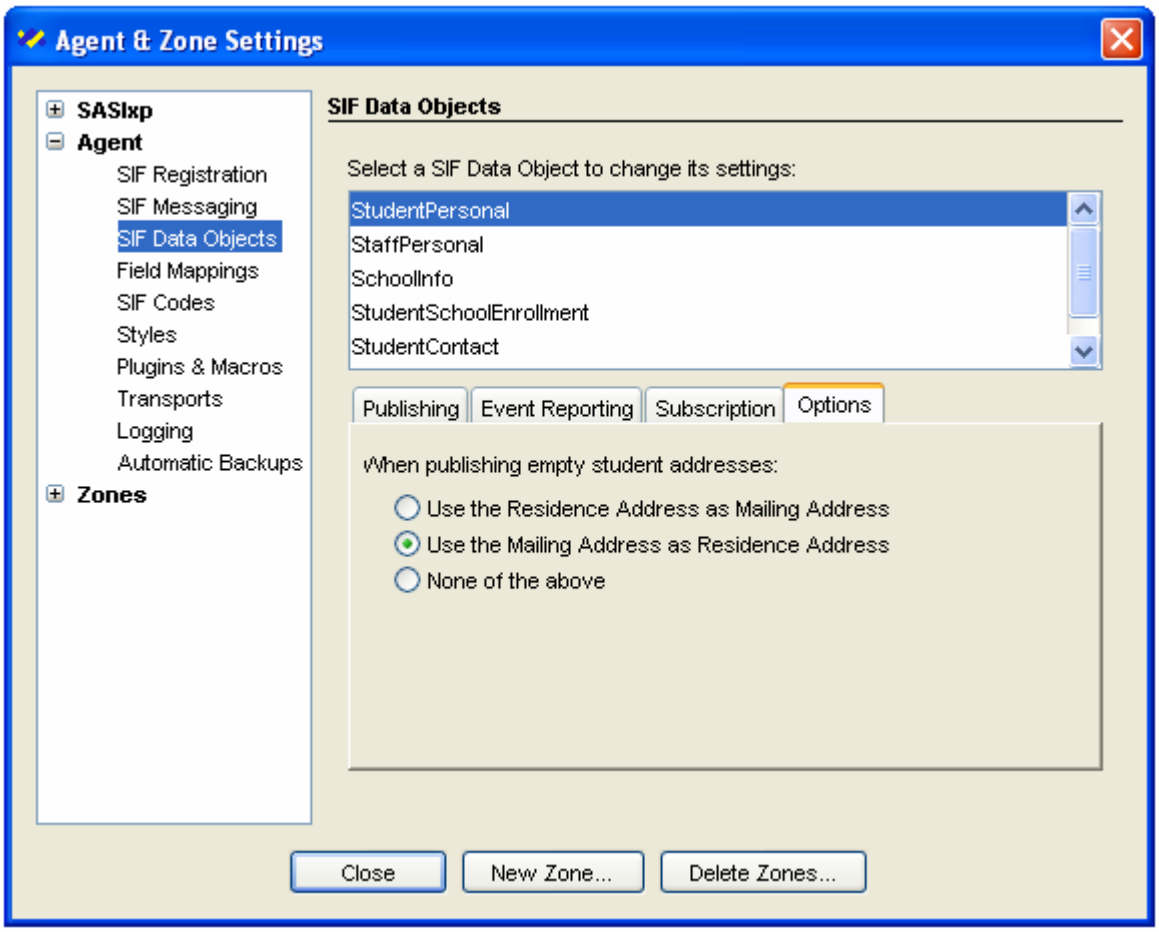
You can improve overall performance of the agent and decrease the size of the SASIxp Event Transaction Log file by setting these checkboxes to match the Access Control permissions at the zone integration server. For example, if the administrator has denied the SASIxp agent permission to report Delete events for students, disable this type of event for StudentPersonal objects. This will result in a more efficient configuration because the agent will not attempt to report events that will be denied by the zone integration server.

Subscription Tab

This release of the SASIxp agent does not support Subscription, but the tab is still visible as a placeholder.

StudentPersonal Options Tab

When StudentPersonal is selected, an Options tab is displayed:



These options can be used to ensure that both a Mailing Address and a Residence Address are published for all students even when one address is blank in SASIxp's database. For example, most transportation systems require a Residence Address in order to properly construct each student's bus route information. However, because Mailing Address is the default for SASIxp, many districts to not type in both a Mailing Address *and* a Residence Address when enrolling students unless the two addresses differ. To force the agent to copy the fields of the Mailing Address into the Residence Address whenever the latter is blank, select the second radio button, "Use the Mailing Address as Residence Address".

Note these options do not modify or otherwise affect student records in the SASIxp database—they only influence the publishing of data by SIF. Refer to the Edustruc-

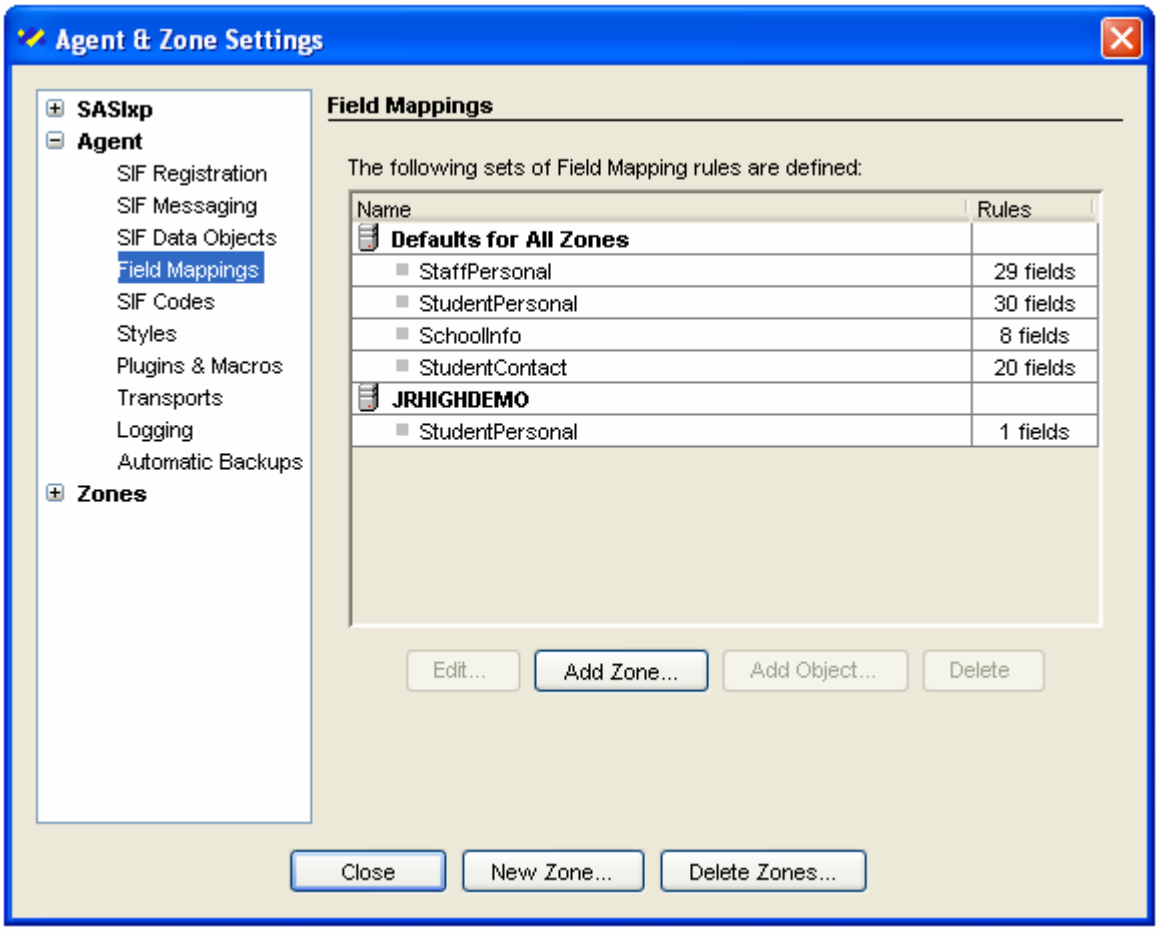
tures Technical Note available from our website for more information about using these options.

Field Mappings

One of the more powerful features of the Edustructures SIF Agent for SASIxp is its flexibility in customizing the way SIF Data Objects are produced from fields in the SASIxp database. In general, any built-in or user-defined field in a SASIxp database table can be *mapped* to an element or attribute in a SIF Data Object.

The agent's factory default mappings are appropriate for most installations. In some cases, however, you will need to fine-tune these mappings to publish additional fields, to change the default SIF Codes assigned to elements such as student IDs, addresses, and telephone numbers, or to adjust the mappings to accommodate a subscriber agent with rigid data-mapping requirements.

Refer to the **Error! Reference source not found.** section in the Advanced Configuration chapter for more information about customizing the agent's field mappings to meet specific integration requirements. Also refer to the Plug-Ins & Macros section later in this chapter.



Field Mapping Rules Summary

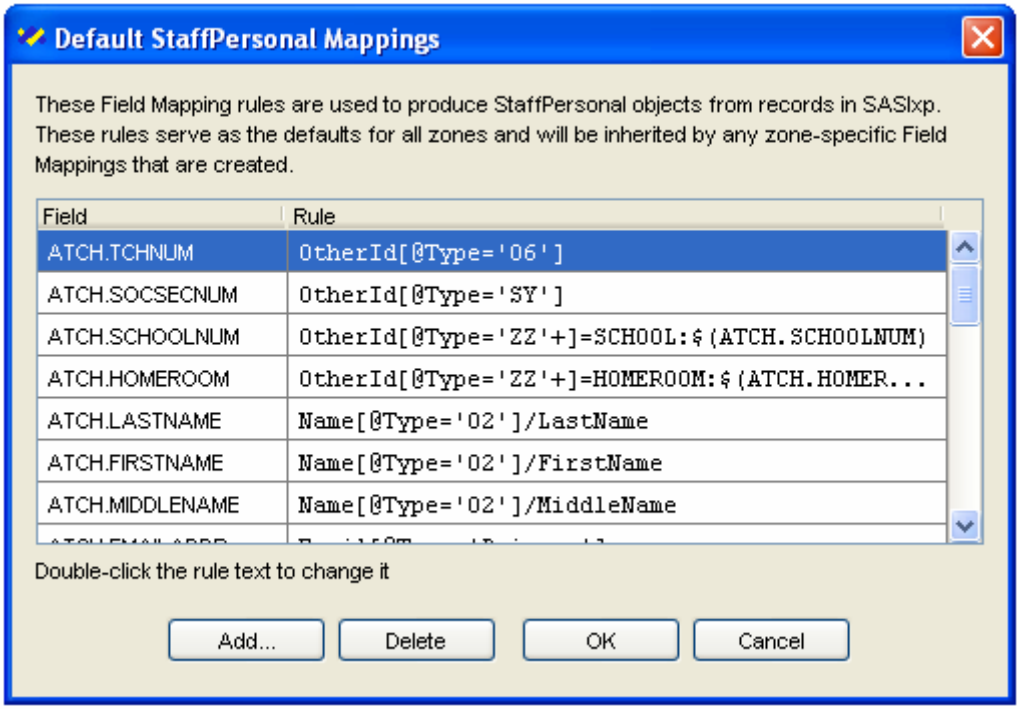
The Field Mappings panel lists each SIF Data Object supported by the agent. A few object types like StudentSchoolEnrollment cannot be customized because they are produced from calculations made by the agent instead of a one-to-one mapping with SASIxp data files and fields. Most SIF Data Objects, however, are customizable and will appear in the list. Defaults for all zones are shown at the top of the list, followed by zone-specific entries.

Field Mapping rules may be modified on a zone-by-zone basis. For example, it is common for elementary school zones to have slightly different mappings than high school zones. In this case, the list will include groups for each zone with indented entries for each customized SIF Data Object. (In the illustration above, one field of the StudentPersonal object has been customized in the JRHIGHDEMO zone. All other field mappings in this zone inherit from the agent defaults.)

How to Change Field Mappings for a SIF Data Object

To change the field mappings for an object,

1. Highlight the object under the "Defaults for All Zones" entry
2. Click the Edit button
3. The following dialog box appears:



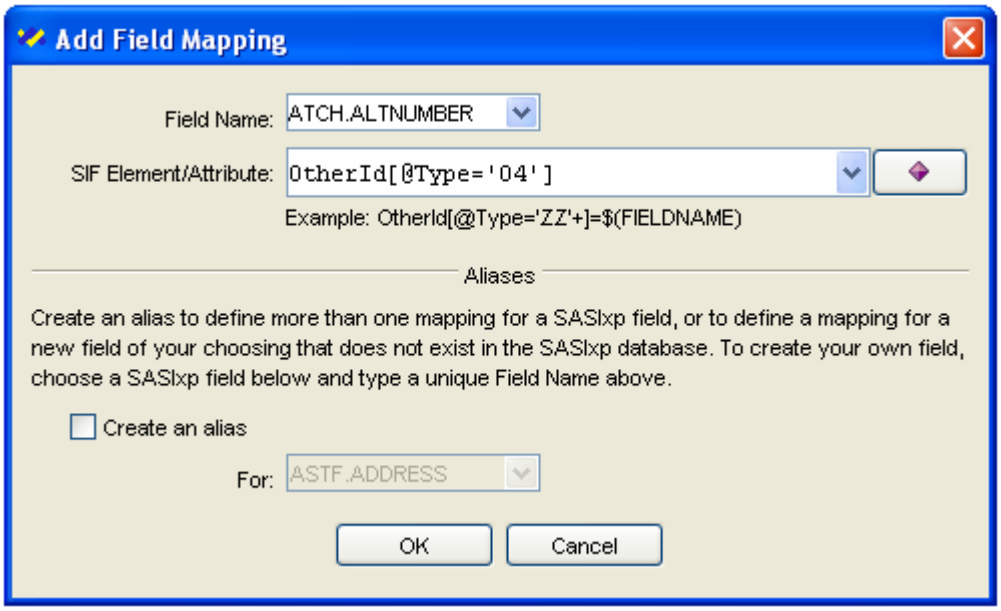
This dialog box lists all field mapping rules for the selected object type. The "Field" column shows the name of a SASIxp data field, and the "Rule" column shows the cor-

responding rule for producing a SIF element or attribute. The SASIxp agent uses rule syntax similar to XPath to describe how to create a SIF element or attribute. Refer to the Mappings section in the Advanced Configuration chapter for details.

To add a new rule,

1. Click the Add button

2. The following dialog box appears:



3. Choose an available field from the "Field Name" combo-box.

   Note: If you're mapping more than one SIF element or attribute to the same SASIxp field, you will need to type in a field name of your choosing that is unique. Each field must have a unique name.

4. Type the mapping rule in the "SIF Element/Attribute" field.

   ▸ **TIP:** To model your entry after an existing one, click the combo-box arrow and choose an existing entry from the menu. To view the macros that can be used in your mapping rule, click the button with the purple diamond.

5. If you're mapping more than one SIF element or attribute to the same SASIxp field, enable the "Create an Alias" checkbox and choose the actual SASIxp field to which this field is mapped. Otherwise, leave this checkbox cleared.

6. Click OK to add the new rule to the SIF Data Object

The above example instructs the SASIxp agent to produce the following element for StaffPersonal objects, using the value of the `ATCH.ALTNUMBER` database field as the element's value:

```
<OtherId Type='04'>Value of ATCH.ALTNUMBER</OtherId>
```

How to Customize Field Mappings for a Zone

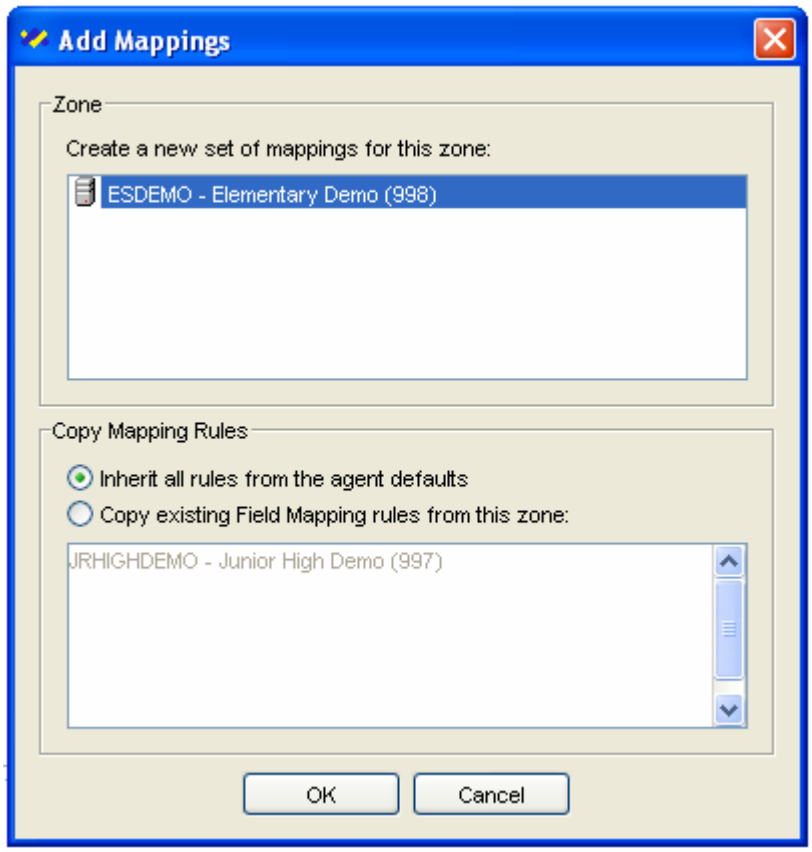
When the SASIxp agent produces a SIF Data Object during Event Reporting or Publishing operations, it first applies any field mapping rules that have been customized for the associated zone. Next, it applies the agent's defaults mapping rules. Thus, you can add new field mappings or "override" one or more of the defaults on a zone-by-zone basis to meet integration requirements that differ from school to school.

For example, in an elementary school zone you might publish the student "advisor" or "counselor" field to a StudentPersonal "OtherId" element, but in a high school zone publish the name of the first period teacher. Since determining the first period teacher of a student requires access to Scheduling-related data files, increasing the amount of time it takes to process each record, the high schools' mapping rules would not be appropriate as agent defaults. They would only be customized for zones representing high schools.

Follow these steps to add a zone-specific field mapping or to "override" a default mapping in a specific zone:

1. From the Field Mappings panel, click the Add Zone button

2. The following dialog box appears



3. Choose the zone to customize from the "Zone" group at the top of the dialog box.

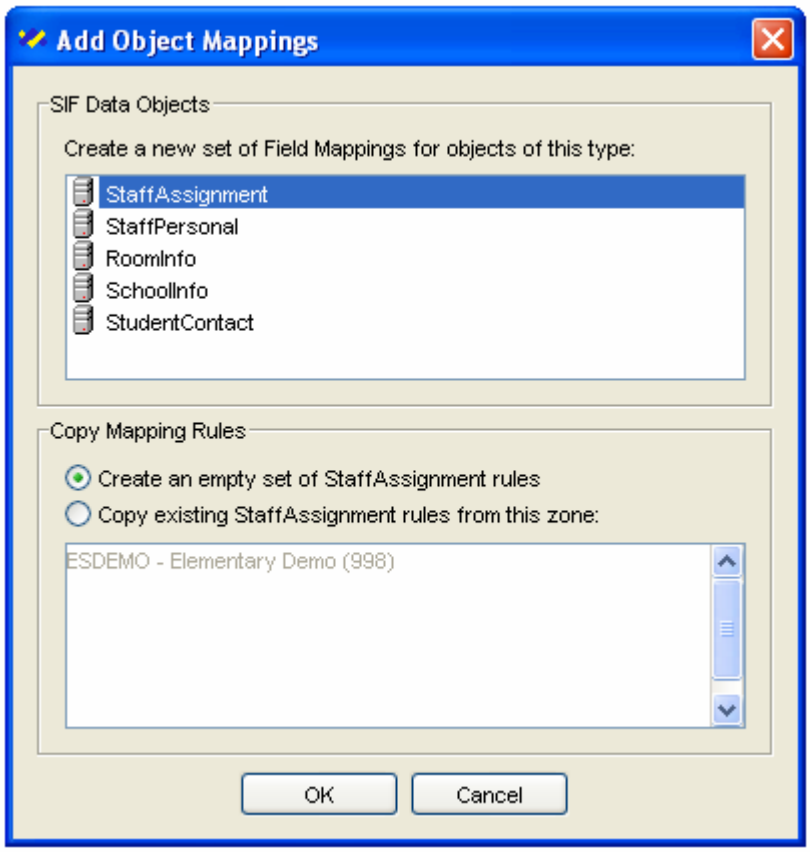
4. To copy mapping rules from another zone, click the "Copy existing Field Mapping rules from this zone" radio button and choose a zone. This option saves time and ensures consistency when creating mapping rules for a group of like zones.

5. Click the OK button to create the new zone group in the Field Mappings panel

To add field mappings for additional SIF Data Objects to your new zone group,

1. Select the new zone group in the Field Mappings panel and click the Add Object button

2. The following dialog box appears:



3. Choose a SIF Data Object from the list

You can now edit the individual field mapping rules for the selected object type as described earlier in this section.

Again, refer to the **Error! Reference source not found.** section in the Advanced Configuration chapter for more information about customizing the agent's field mappings to meet specific integration requirements.

SIF Codes

The Schools Interoperability Framework standard defines a consistent set of codes that are used for fields such as Grade Level, Ethnicity, Language, and English Proficiency. Each application must translate its own application-defined codes to these SIF-defined codes so that all agents participating in a zone agree on a common set of values. The **SIF Codes** group of settings allows you to customize the SASIxp-to-SIF translation tables that are used by the agent when it publishes data to a zone.

The original SIF specification used codes from the SPEEDE/ExPRESS standard, while SIF 1.1 and later prefers NCES codes. Refer to the SIF Specification (available from the www.sifinfo.org website) for a complete list. Although you can change the SASIxp agent to use either set of codes, the factory defaults reflect the SPEEDE standard to

enable the agent to more easily interoperate with older SIF 1.0r1 zones. In a future release of the agent, the factory defaults will reflect the newer NCES codes.

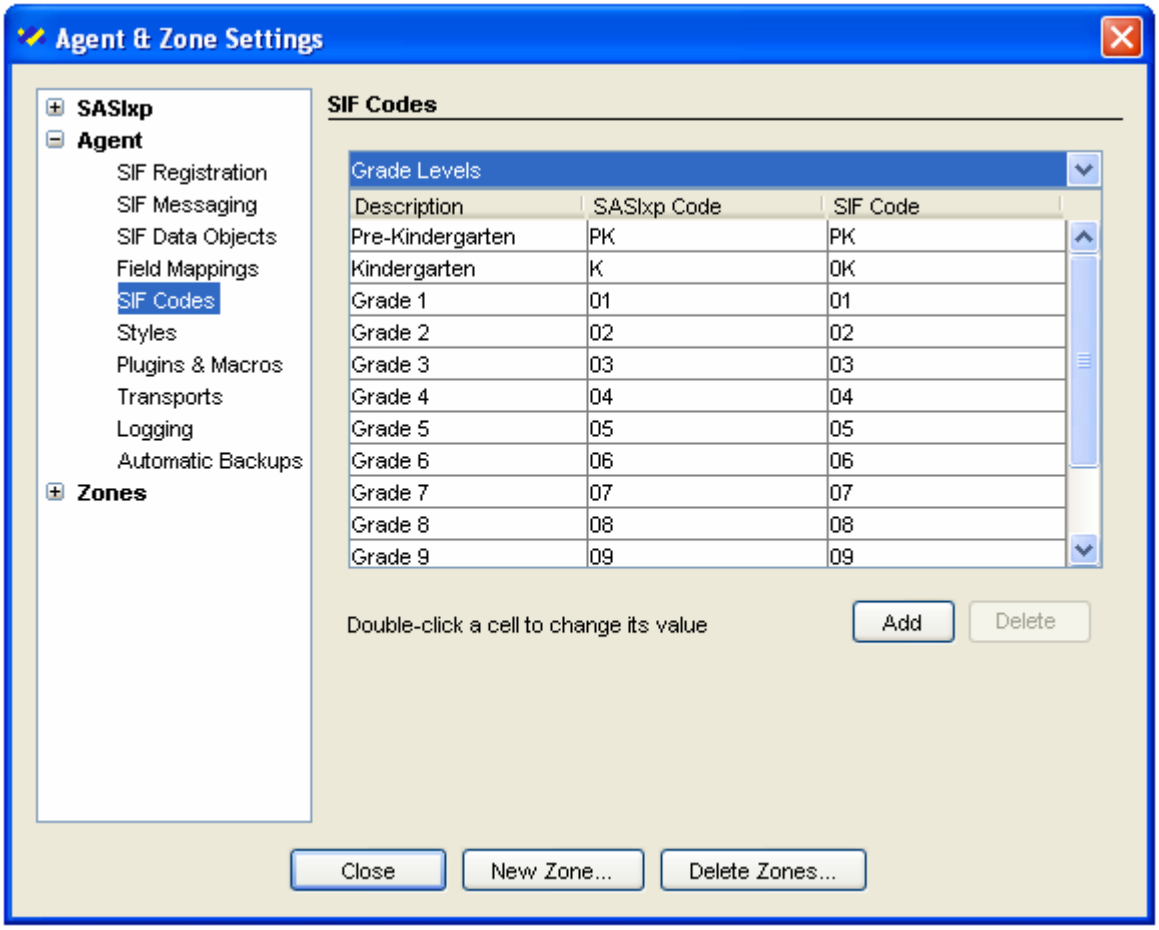
Before connecting the agent to the zone integration server, it is a good idea to verify that the factory default codes are appropriate for your district. Since codes such as Grade Level and Ethnicity are customizable in SASIxp, it is usually necessary to configure the agent's SIF Codes to reflect the specific SASIxp values used at your district. For example, if your district uses "K" to represent the Kindergarten grade instead of the factory default of "00", the Grade Levels table must be changed to reflect this.

Grade Levels

To edit the Grade Levels table,

1. Click the **SIF Codes** node in the tree

2. Choose "Grade Levels" from the combo-box at the top of the page



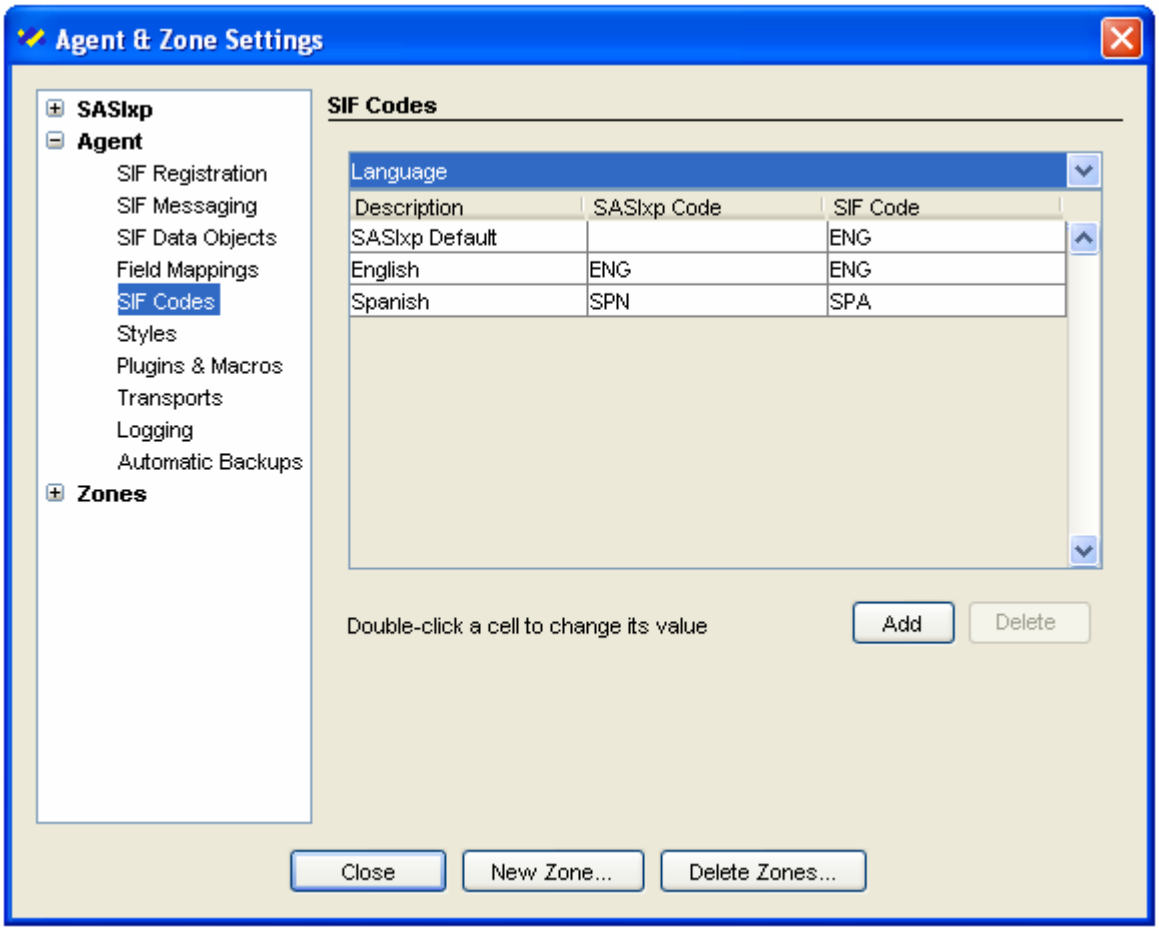
3. Double-click any value in the SASIxp Code column to change a grade level to match the values used at your district

Language

To edit the Language table,

1. Click the **SIF Codes** node in the tree

2. Choose "Language" from the combo-box at the top of the page



3. Double-click any value in the SASIxp Code column to change a language code to match the values used at your district

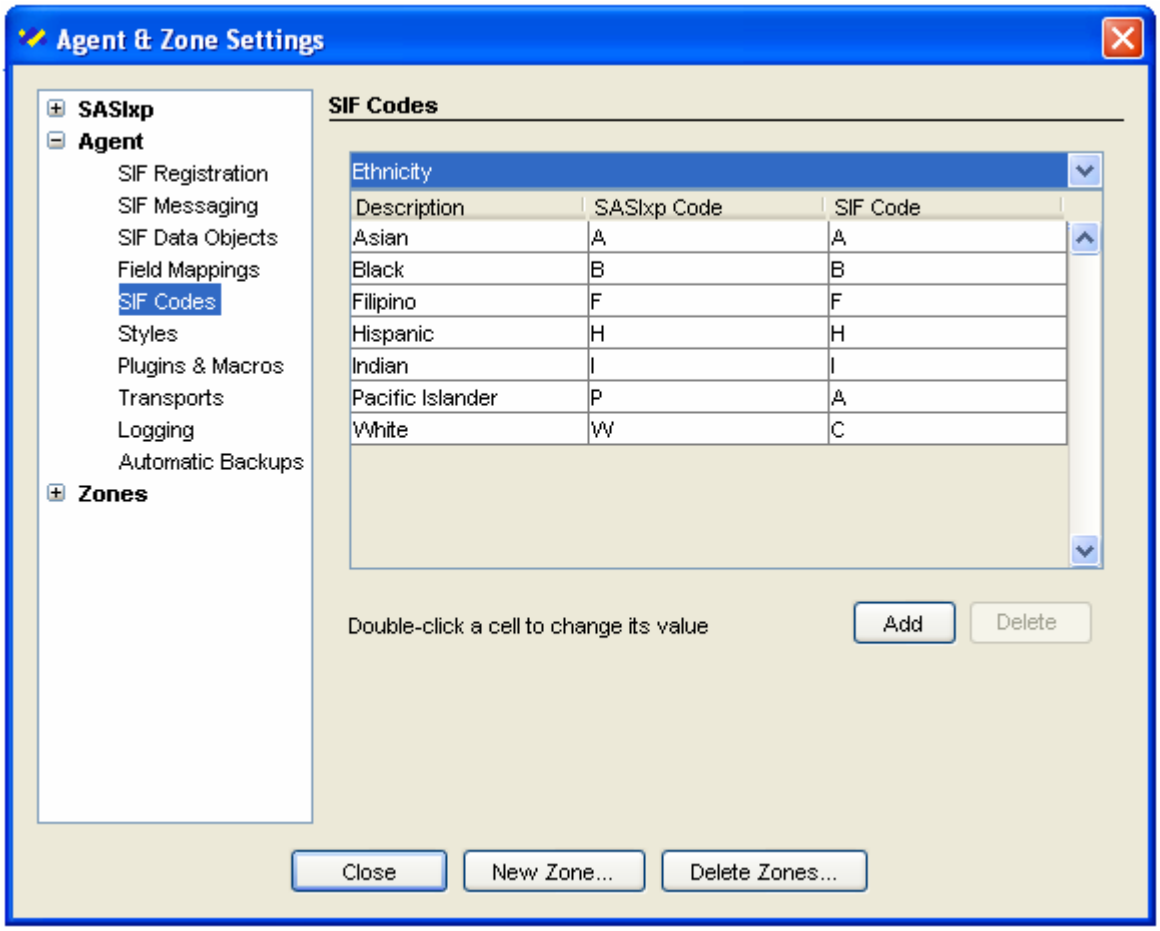
4. To add a Language, click the Add button and enter both the SASIxp Code and the equivalent SIF Code. The new entry is appended to the end of the list (order is not important to the functionality of the agent.) To delete a code, select it in the list and click the Delete button.

Ethnicity

To edit the Ethnicity table,

1. Click the **SIF Codes** node in the tree

2. Choose “Ethnicity” from the combo-box at the top of the page



3. Double-click any value in the SASIxp Code column to change an Ethnicity code to match the values used at your district

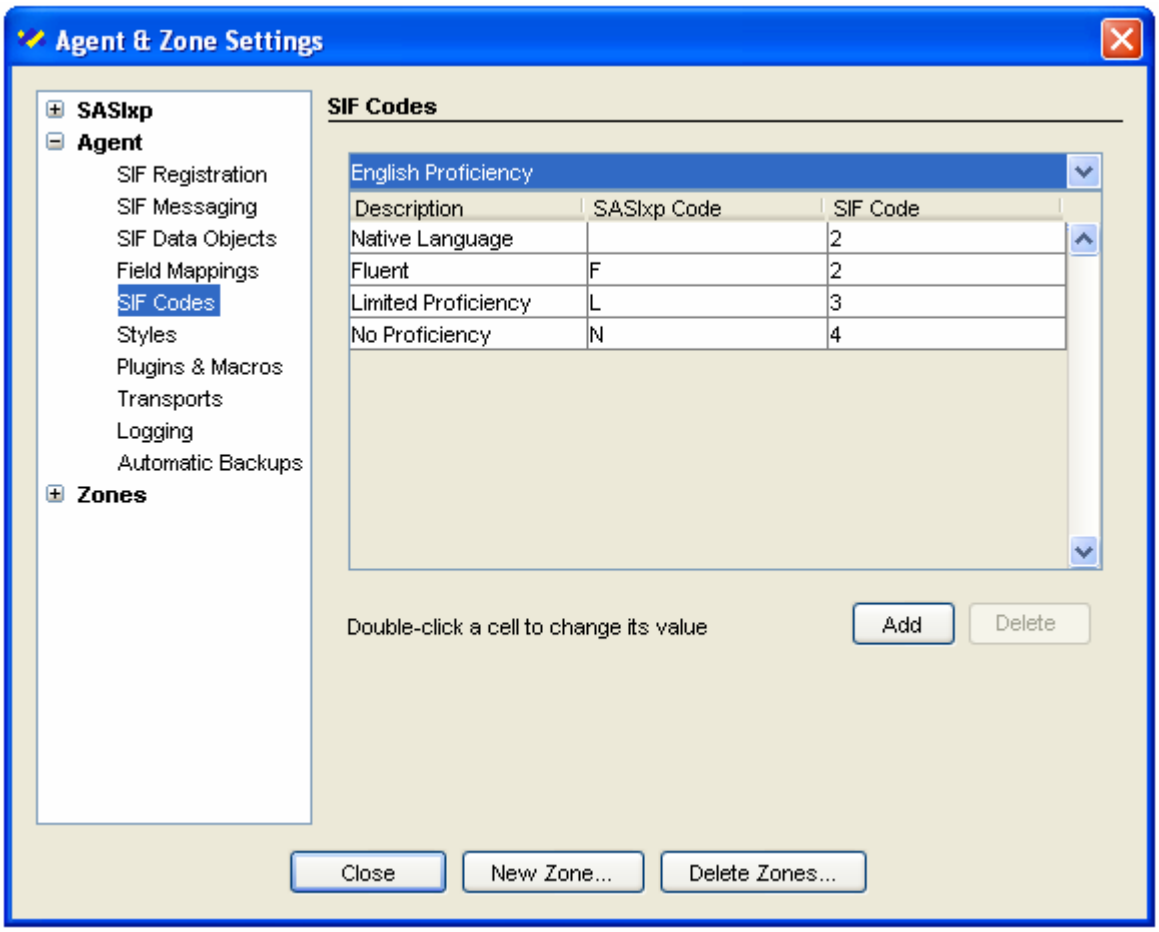
4. To add an Ethnicity code, click the Add button and enter both the SASIxp Code and the equivalent SIF Code. The new entry is appended to the end of the list (order is not important to the functionality of the agent.) To delete a code, select it in the list and click the Delete button.

English Proficiency

To edit the English Proficiency table,

1. Click the **SIF Codes** node in the tree

2. Choose “English Proficiency” from the combo-box at the top of the page



3. Double-click any value in the SASIxp Code column to change an English Proficiency code to match the values used at your district. Note that two or more SASIxp English Proficiency codes may translate to the same SIF Code value.

4. To add an English Proficiency code, click the Add button and enter both the SASIxp Code and the equivalent SIF Code. The new entry is appended to the end of the list (order is not important to the functionality of the agent.) To delete a code, select it in the list and click the Delete button.

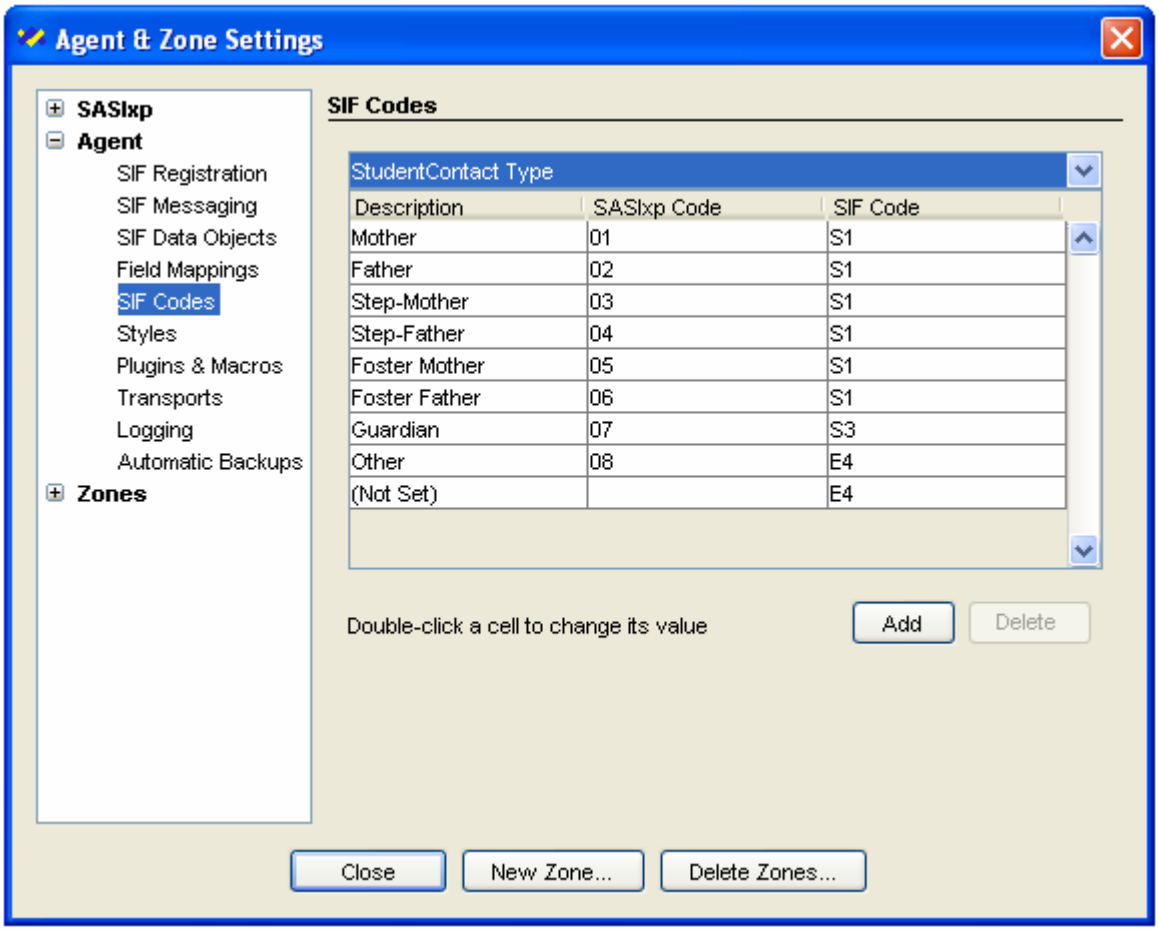
StudentContact Type and Relationship

The SIF `StudentContact` data object includes both a Type and a Relationship code field, each of which uses an independent set of codes defined by the SIF Specification. The "StudentContact Type" and "StudentContact Relationship" tables let you define how the SASIxp Parent/Guardian relationship code translates to these two fields.

Note that these tables may have many entries that translate to the same SIF code. For example, the SASIxp relationship codes for Mother, Father, Step-Mother, and Step-Father all translate to a single StudentContact Type of "S1", defined by the SIF Specification as "Parent".

1. Click the **SIF Codes** node in the tree

2. Choose "StudentContact Type" or "StudentContact Relationship" from the combo-box at the top of the page



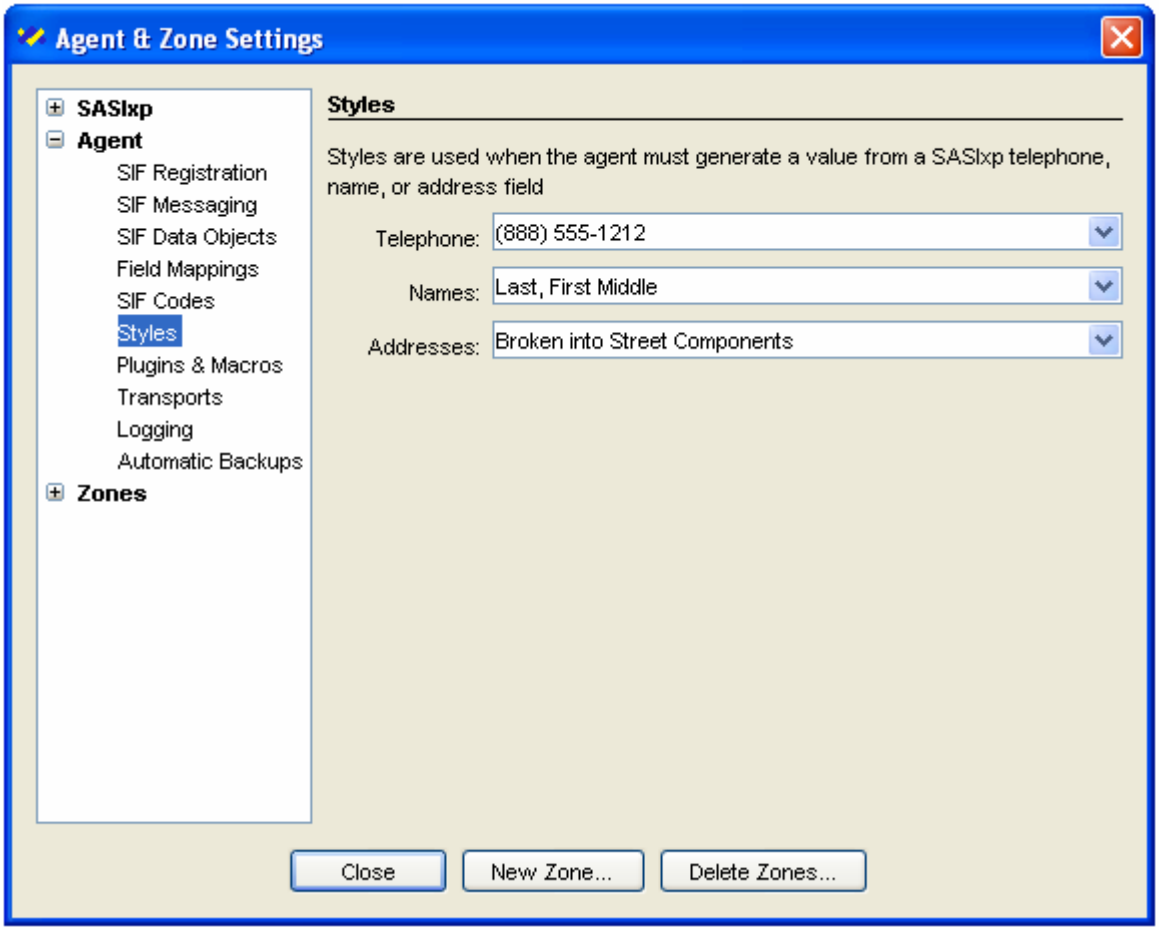
3. Double-click any value in the SASIxp Code column to change a language code to match the values used at your district. Note that two or more SASIxp English Proficiency codes may have the same SIF Code value.

4. To add a code code, click the Add button and enter both the SASIxp Code and the equivalent SIF Code. The new entry is appended to the end of the list (order is not important to the functionality of the agent.) To delete a code, select it in the list and click the Delete button.

Style Settings

Style settings control how the agent formats telephone numbers, person names, and addresses whenever it must produce a value of this type. For example, telephone numbers are actually stored as unformatted numbers (e.g. 8017901261 versus "801-790-1261") in the SASIxp database. Whenever the agent populates a SIF telephone

number field with a value from the database, it consults the Style settings to determine how to format the number as a string.



Telephone

This style defines how telephone numbers are formatted (e.g. “801-790-1261”)

Names

This style defines how person names are formatted (e.g. “Last, First M”)

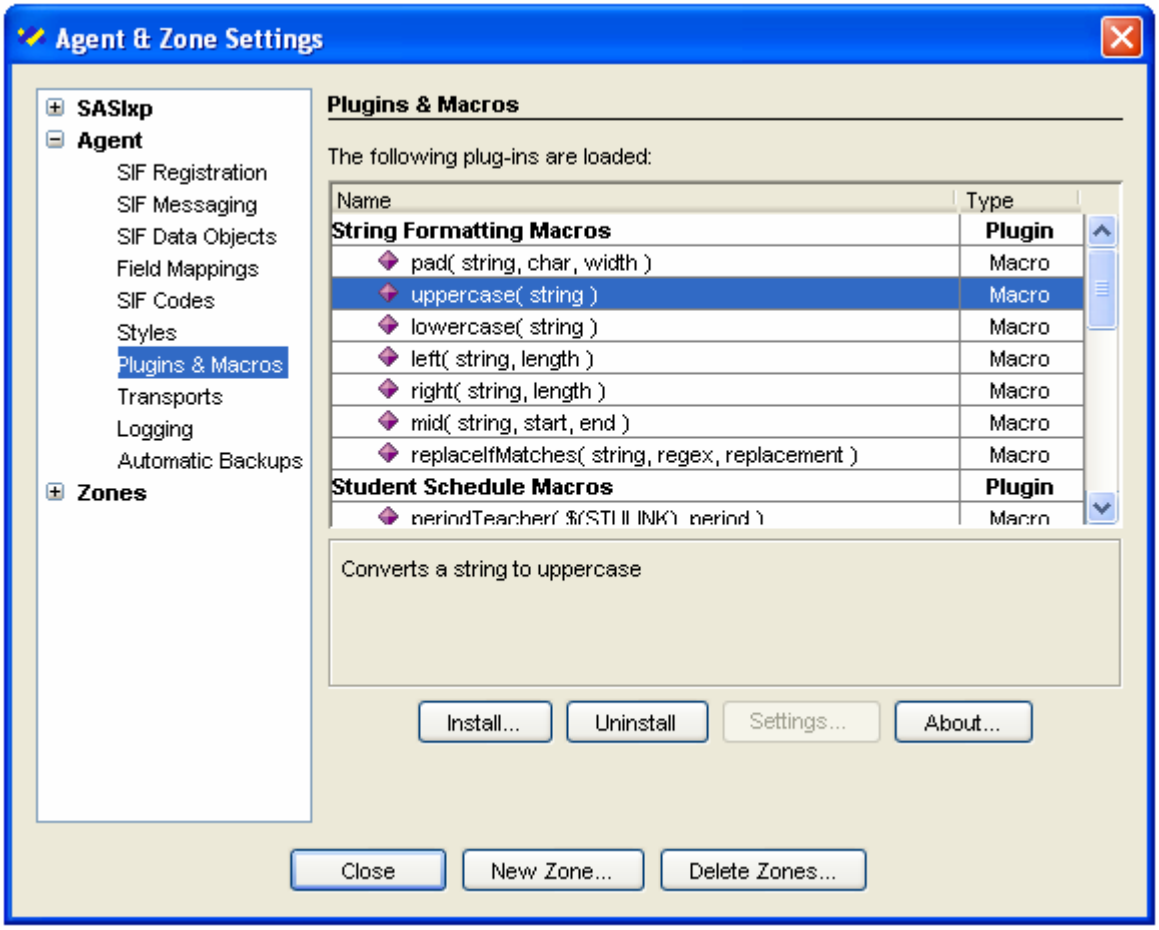
Addresses

This style indicates whether addresses should be published as they’re stored in the SASIxp database (i.e. as simple strings), or broken into individual address elements. The latter is most useful for integration with transportation systems that recognize the individual components of an address (i.e. direction, street number, street name, apartment or building number, and so on.)

Plug-Ins & Macros

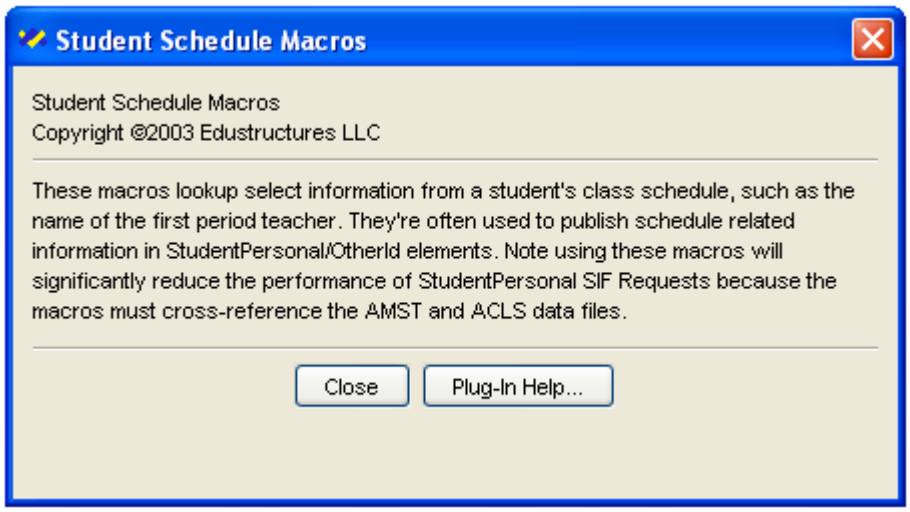
The Plug-Ins & Macros panel shows the various *plug-in modules* that are loaded by the SASIxp agent, and the *macros* contained in each. Use this panel to install and uninstall plug-ins modules from Edustructures and third-party companies. The agent includes several plug-ins, some of which are installed by default and others that must be manually installed as needed.

Macros are used in field mappings to perform calculations and cross-table database lookups when the agent converts field data from SASIxp to SIF Data Object form. Refer to the **Error! Reference source not found.** section in the Advanced Configuration chapter for details.



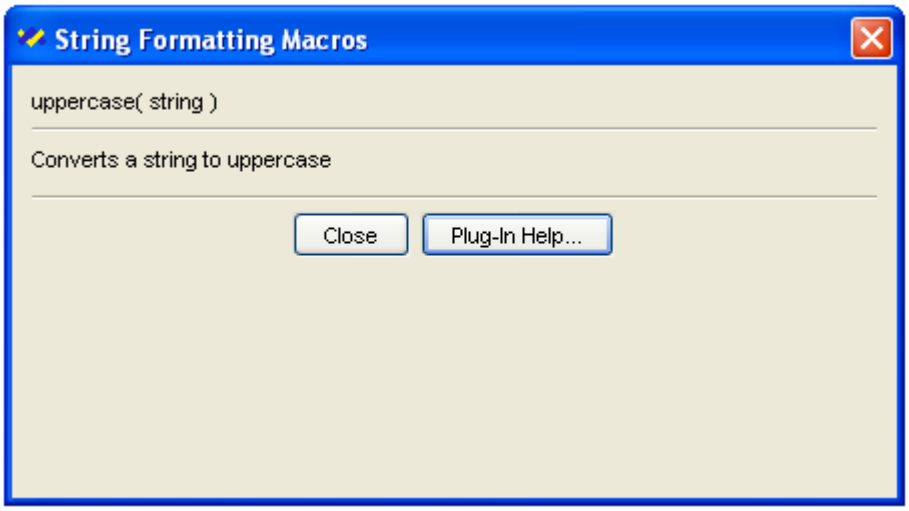
Reviewing Loaded Plug-Ins & Macros

The Plug-Ins & Macros page displays all plug-in modules that are currently loaded. A description of the highlighted entry is displayed beneath the table. You can also click the About button to open a dialog box with more information.



For plug-in modules, the About dialog box shows the name of the plug-in, the author's copyright notice, and a brief description of the plug-in module's contents. Some plug-ins provide additional documentation and help pages on the web. If available, the Plug-In Help button if visible.

For macros, the About dialog box shows the syntax of the macro (i.e. the number of parameters and the name of each) as well as a brief description of the macro's purpose:

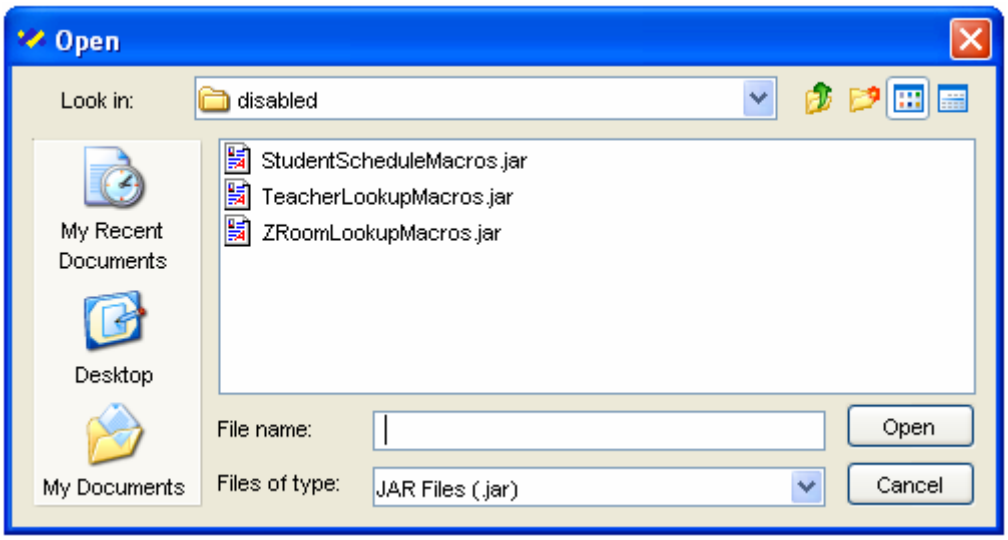


Installing a Plug-In Module

Follow these steps to install a plug-in module:

1. Click the Install… button

2. Choose a plug-in file from the agent's "/plugins/disabled" directory. If you downloaded a plug-in from Edustructures or a third-party company, use the dialog box to navigate to the plug-in's JAR file.



▸ **IMPORTANT:** Some plug-in modules are dependent on others in order to work properly. For example, the Room Lookup Macros require that the Teacher Lookup Macros also be installed (although the reverse is not true). This dependency is documented in the About dialog box that's displayed for the Room Lookup Macros plug-in.

In addition, some macros cache information from SASIxp for each zone the agent is connected to and therefore increase the amount of time it takes for the agent to start up. For this reason, it is recommended that you only install those plug-in modules that you're making use of in Field Mappings. Performance considerations are usually documented in the plug-in module's About dialog box.

After installing a plug-in, review the About dialog box to make sure you understand any performance implications and/or dependencies the plug-in has on other modules.

Uninstalling a Plug-In Module

To remove a plug-in module,

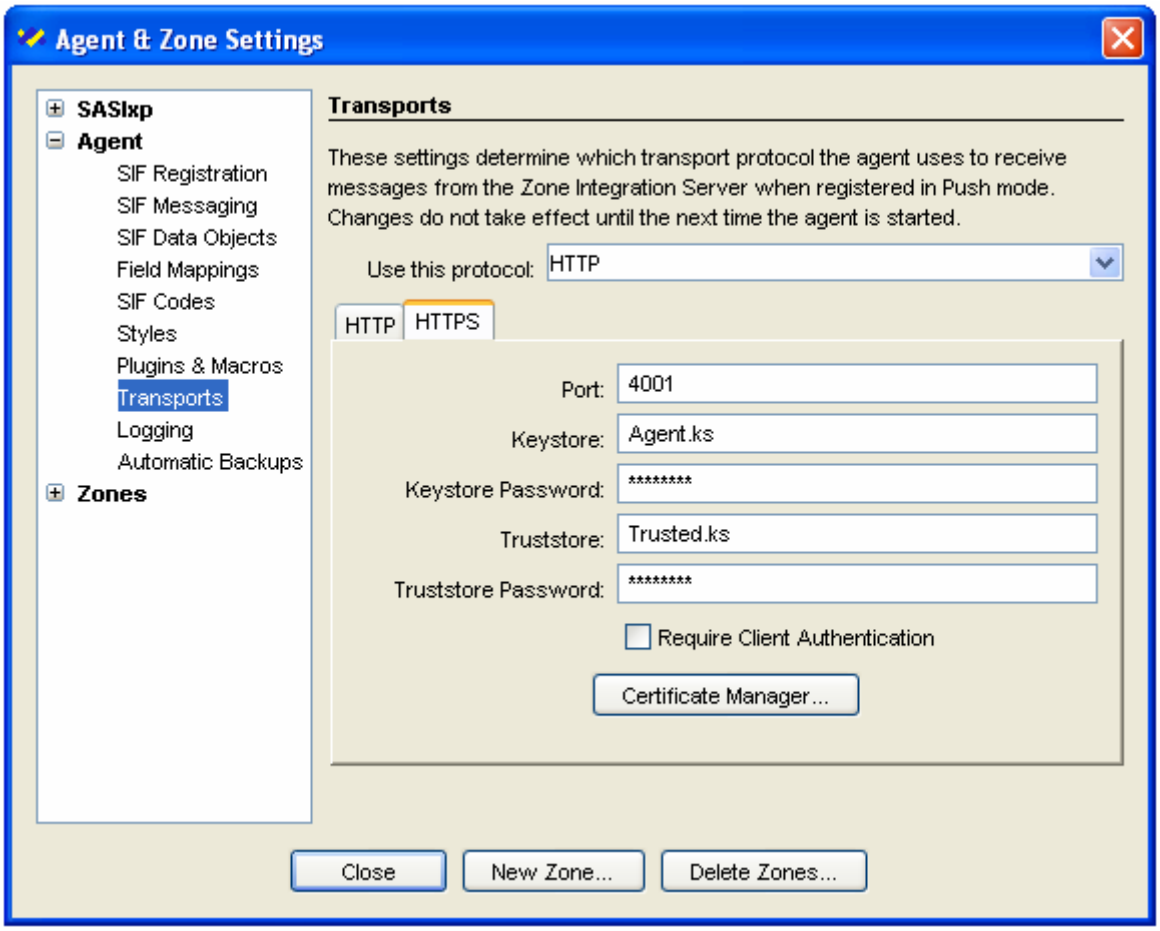
1. Select the plug-in from the list

2. Click the Uninstall button

The plug-in module is unloaded and its JAR file is moved from the agent's "/plugins" directory to the "/plugins/disabled" directory.

Transport Settings

The Transports group of settings controls how the agent communicates with the zone integration server over the HTTP or HTTPS transport protocols. Refer to the Security section in the Advanced Configuration chapter for additional information on configuring HTTPS.



Protocol

Choose the networking protocol used to communicate with the zone integration server when the agent is running in Push mode. (In Pull mode, this setting is ignored.) The default is HTTP. When the agent starts up, it will establish a networking socket on the specified port to "listen" for incoming messages sent by the zone integration server.

▸ **NOTE:** The protocol chosen here must match the protocol used in the Zone URL field of each zone. (See Zone Configuration later in this chapter.) In other words, you cannot send messages to the ZIS over HTTPS but configure the Transports settings to receive messages over HTTP. The protocols must match.

HTTP Port

The port the agent will listen on for incoming HTTP traffic when the Protocol field is set to HTTP. The factory default is 4000. Change the port number only if another application on the computer is already using this port.

HTTPS Port

The port the agent will listen on for incoming HTTPS traffic when the Protocol field is set to HTTPS. The factory default is 4001. Change the port number only if another application on the computer is already using this port.

Require Client Authentication

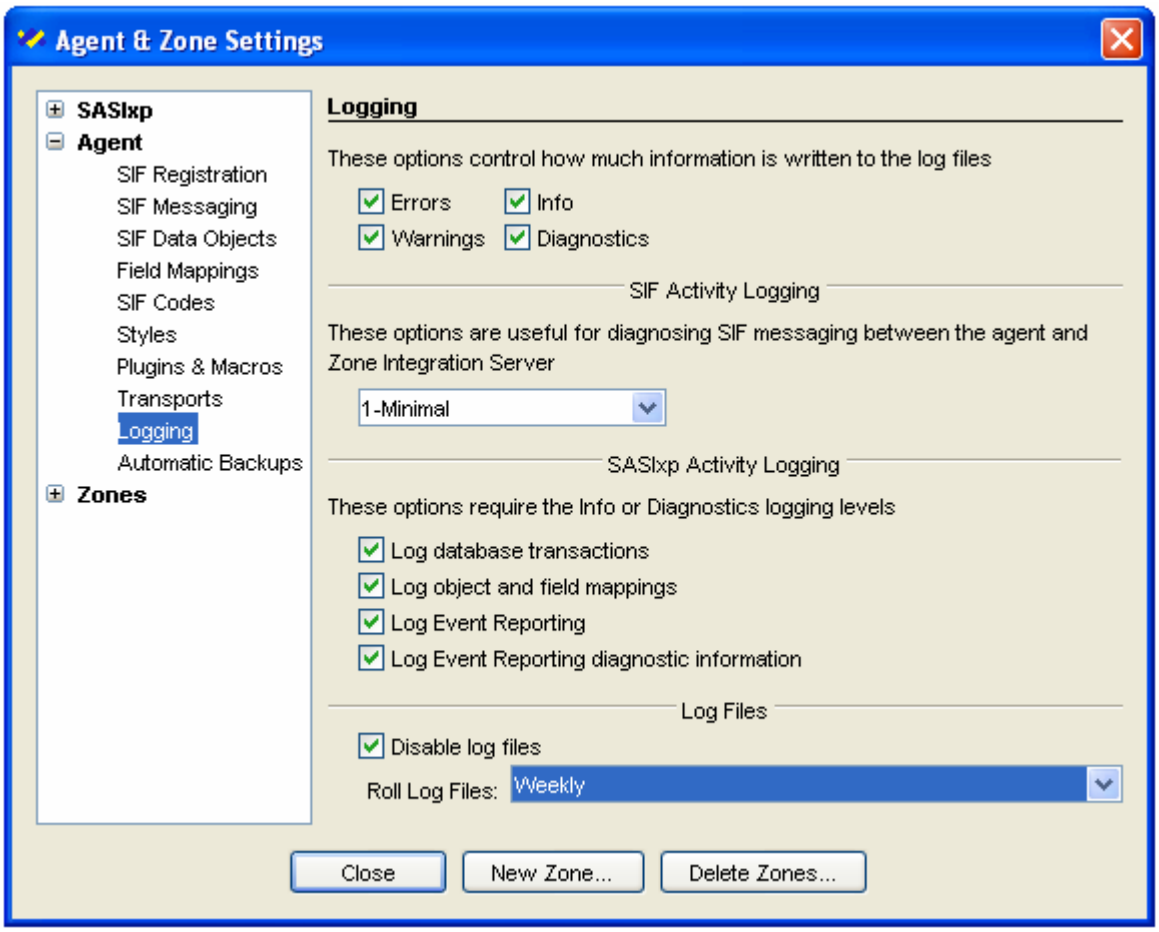
Check this checkbox if the agent should require Client Authentication from the zone integration server when it connects to a zone. In other words, the ZIS must present a valid certificate with a matching host name in order for a connection to be established.

Certificate Manager

Refer to the section of Security in the Advanced Configuration chapter for more information about managing digital certificates for HTTPS connectivity.

Logging Settings

This group of settings controls the amount of diagnostic logging information that is written to the agent and zone logs. Log files are found in the agent's "logs" subdirectory.



Errors, Warnings, Info and Diagnostics

These checkboxes control how much information is written to the log files

SIF Activity Logging

This setting controls how much if any low-level SIF Messaging activity is written to the log files, independent of any SASIxp-related activity. Experiment with these settings to determine how much logging is desired. For example, if you're interested in viewing the actual SIF infrastructure messages that are exchanged between the agent and zone integration server, choose the "4-Detailed" level or higher. If you're only interested in seeing the SIF message identifiers but not the actual payload of each message, decrease the logging level to "2-Moderate". To view all SIF activity logging, choose "6-All".

SASIxp Activity Logging

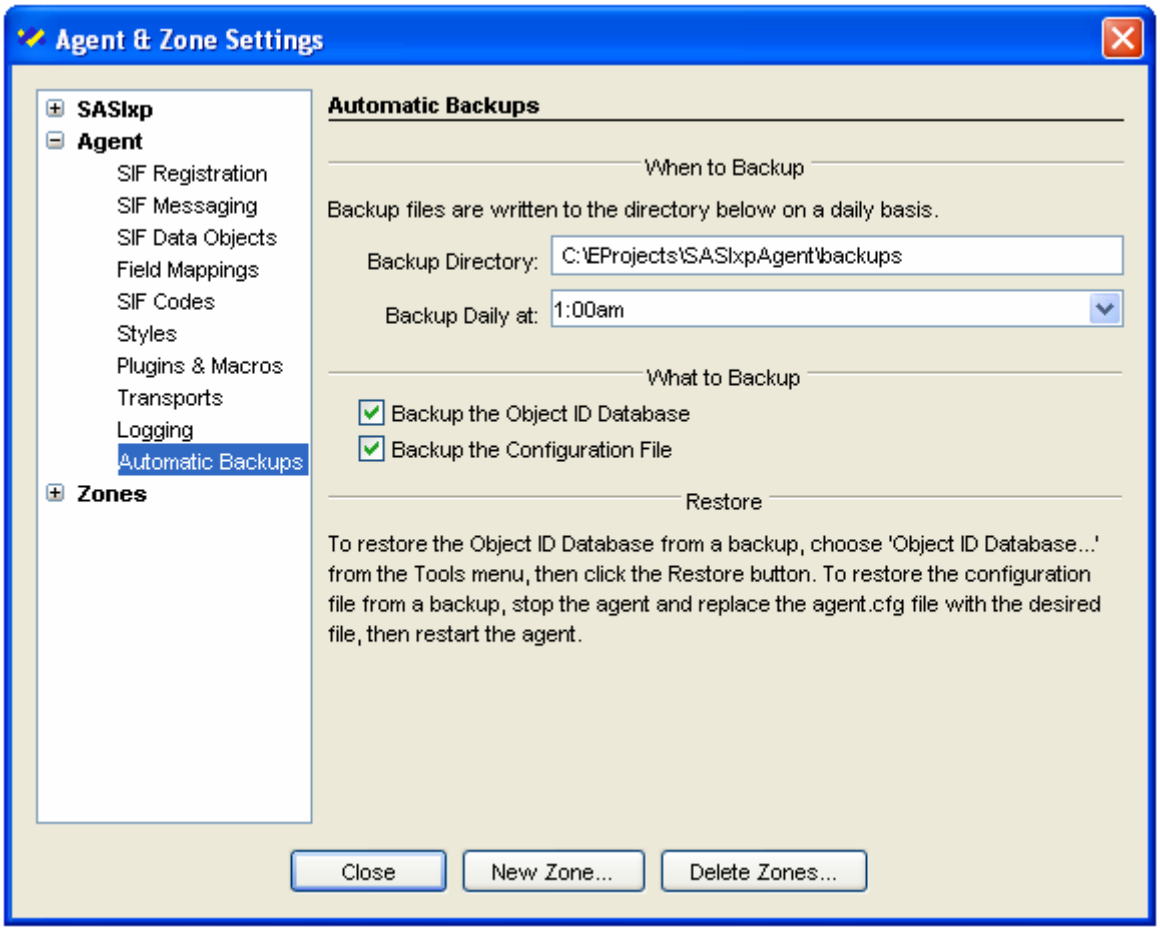
Use these checkboxes to choose the types of SASIxp-related activities that will be written to the log files. For example, to view details about each change captured in the SASIxp Event Transaction Log whenever the agent reports a SIF Event, check the "Log Event Reporting" and "Log Event Reporting Details" check boxes. Note the lat-

ter is considered a *diagnostic* log level so "Diagnostics" checkbox must also be checked at the top of the page.

Automatic Backup Settings

The SASIxp agent can perform automatic backups of both the configuration file and Object ID Database on a nightly basis. Backups are written to the agent's "backups" sub-directory at the time of day selected (by default, 10:00pm). The name of the backup file is numbered 1-7 to reflect the seven days of the week.

By turning on Automatic Backup and including the "backups" directory in your district's regular tape backup plan, you can ensure that both the agent configuration file and Object ID Database are backed up on a nightly basis. Should it become necessary to restore the Object ID Database from a tape backup, use the Restore button on the Object ID Database dialog box available from the Tools menu as described on page 71.



Zone Configuration

The final step in the configuration of the SASIxp agent is to define the SIF Zones to which it will connect.

SIF Zones Overview

The Schools Interoperability Framework features a scalable architecture in which applications and their data are organized into "zones". Each SIF Zone is managed by a zone integration server. When two or more agents register in a zone, they're able to communicate with one another by exchanging messages with the server.

SASIxp School Zones

The data that flows through a zone is defined by the agents that publish data—in the case of SASIxp, the set of records published to each zone comes from a single school. This is because the SASIxp agent employs a "one school per zone" model in which data from each school is published to a zone specifically created for that school (versus publishing the data from all schools in the district to a single, monolithic zone.) This one-school-per-zone approach is the most scalable, flexible method of deploying the Schools Interoperability Framework.

Aggregate Zones

In some cases it is necessary to group two or more schools into a single zone. For example, a State Department or a Regional Service Agency may wish to connect to your SIF infrastructure in order to query SIF Data Objects for the purpose of vertical reporting. It would be cumbersome for this kind of application to connect to each school zone individually, especially in a large district. What's needed is a way for the district administrator to create a single, monolithic zone that represents all schools in the district. This way, the State Department can connect to one zone instead of tens or hundreds of school zones.

With the SASIxp agent, you can create "aggregate zones" that serve to aggregate the data from two or more school zones. Aggregate zones function as a single point of communication for many school zones. When a SIF Request is received, it is dispatched to all of the school zones that are members of the Aggregate Zone; the results are combined into a single response and returned to the requesting agent. Similarly, when events are reported by a SASIxp school, they're also reported to any Aggregate Zones of which the school is a member.

Creating School Zones

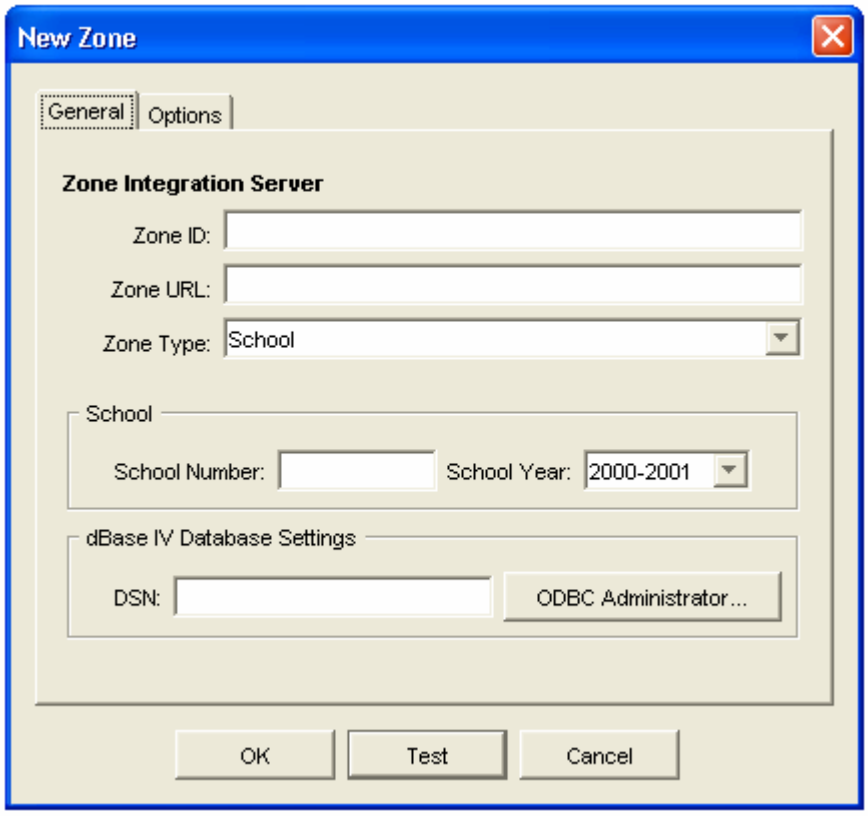
SIF Zones are defined and managed by a Zone Integration Server, not by the SASIxp agent. Before you can configure the agent to connect to a zone, that zone must first be created and configured at the SIFWorks® Zone Integration Server.

Before proceeding, gather the following information:

- The IP address or hostname of the SIFWorks ZIS
- The protocol used by the SIFWorks ZIS (e.g. HTTP or HTTPS)
- The port number of the SIFWorks ZIS (7080 is the default)
- The Zone ID (e.g. "CLEMENTS_MS")

Next, follow these steps to define each school zone to which the agent will connect:

1. Start the agent if not already running
2. Click on the SIF logo on the system tray to open the Console
3. Choose **Settings** from the Tools menu
4. Click the **New Zone…** button
5. The New Zone dialog box will appear:



6. Fill in the Zone Integration Server fields:

Field	Description
Zone ID	The ID of the zone. This value is case-sensitive and must precisely match the zone ID on the zone integration server that manages this zone
Zone URL	The URL to connect to the zone integration server that manages

	this zone. When connecting to SIFWorks®, the format of the URL is: "http://hostname:port/ZoneID". Note the ZoneID is case sensitive and must be entered exactly as it appears in the SIFWorks ZIS Console.
Zone Type	Choose "School Zone" to create a zone that maps to a SASIxp school. Once you've created two or more school zones, you can choose "Aggregate Zone" to create a special type of zone that serves to aggregates schools zones into a single SIF Zone. Aggregate zones are discussed in greater detail in Part III of this guide.

7. Fill in the school number and school year fields

Field	Description
School Number	The SASIxp school number (e.g. "301")
School Year	The SASIxp school year (e.g. "2002-2003")

8. Fill in the database settings.

   dBASE IV Users: Enter the name of the ODBC System DSN for this school. Refer to *Creating System DSNs for Each School* on page 18 for details.

   Oracle and SQL Server Users: If you're using Oracle or SQL Server, school zones typically connect to a single, centralized database instead of multiple databases. The configuration parameters for this database was specified earlier in the SASIxp Options pane of the Settings dialog box (see page 22). If you want to change the database settings for a specific zone, click the Details button and clear the "Use defaults" checkbox.

9. Click the Test button to test that the zone, school, and database properties are correct. If the agent is able to successfully connect to both the SASIxp database for this school and the Zone Integration Server, a message box will be displayed showing the name of the school. If an error occurs during the test, a message box is displayed with detailed error information.

10. Click OK to save your changes. The new zone is added to the Zones tree in the Agent & Zone Settings dialog box and is also added to the main window of the Console.

Repeat these steps for each SASIxp school zone.

Creating Aggregate Zones

Follow these steps to create an Aggregate Zone:

1. Start the agent if not already running

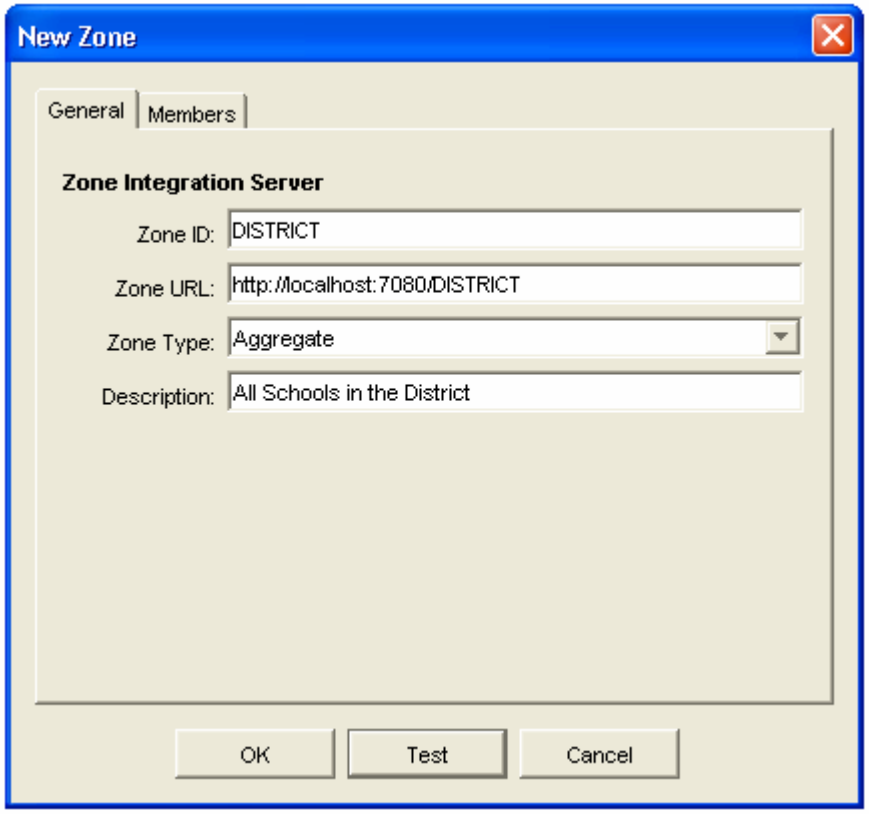
2. Click on the SIF logo on the system tray to open the Console

3. Choose **Settings** from the Tools menu

4. Click the **New Zone…** button

5. The New Zone dialog box will appear

6. Change the Zone Type field to "Aggregate Zone":

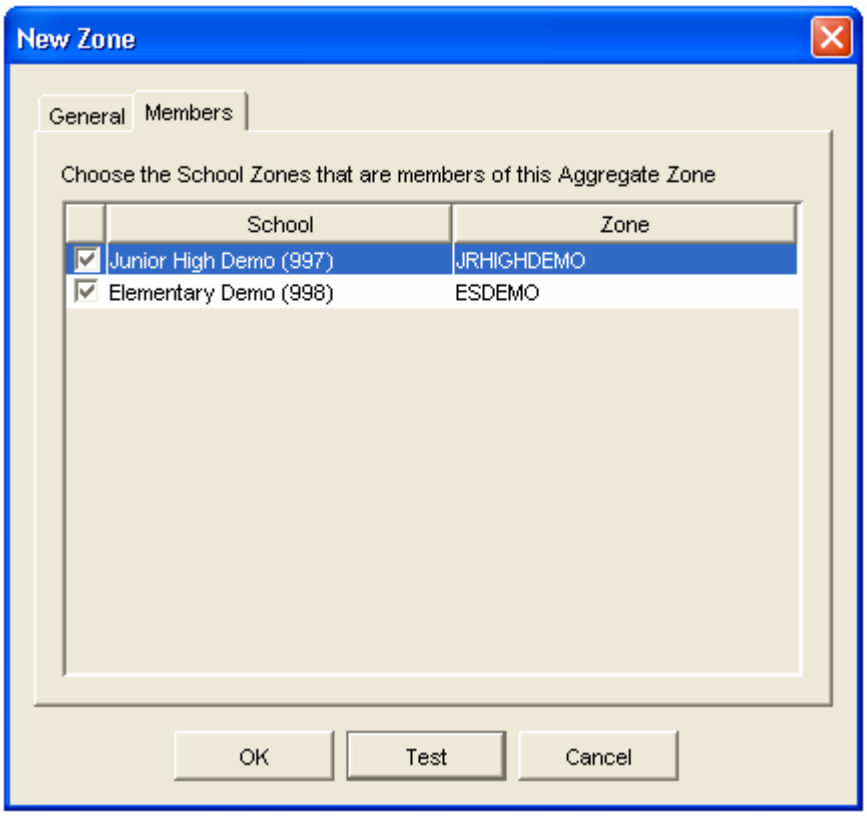


7. Fill in the Zone ID and Zone URL fields

Field	Description
Zone ID	The ID of the zone. This value is case-sensitive and must precisely match the zone ID on the zone integration server that manages this zone
Zone URL	The URL to connect to the zone integration server that manages this zone. When connecting to SIFWorks®, the format of the URL is: "http://hostname:port/ZoneID". Note the ZoneID is case sensitive and must be entered exactly as it appears in the SIFWorks ZIS Console.

8. Type an optional description in the Description field. This text will appear on the Console's main window.

9. Click the Members tab to select the schools that are members of this aggregate zone.

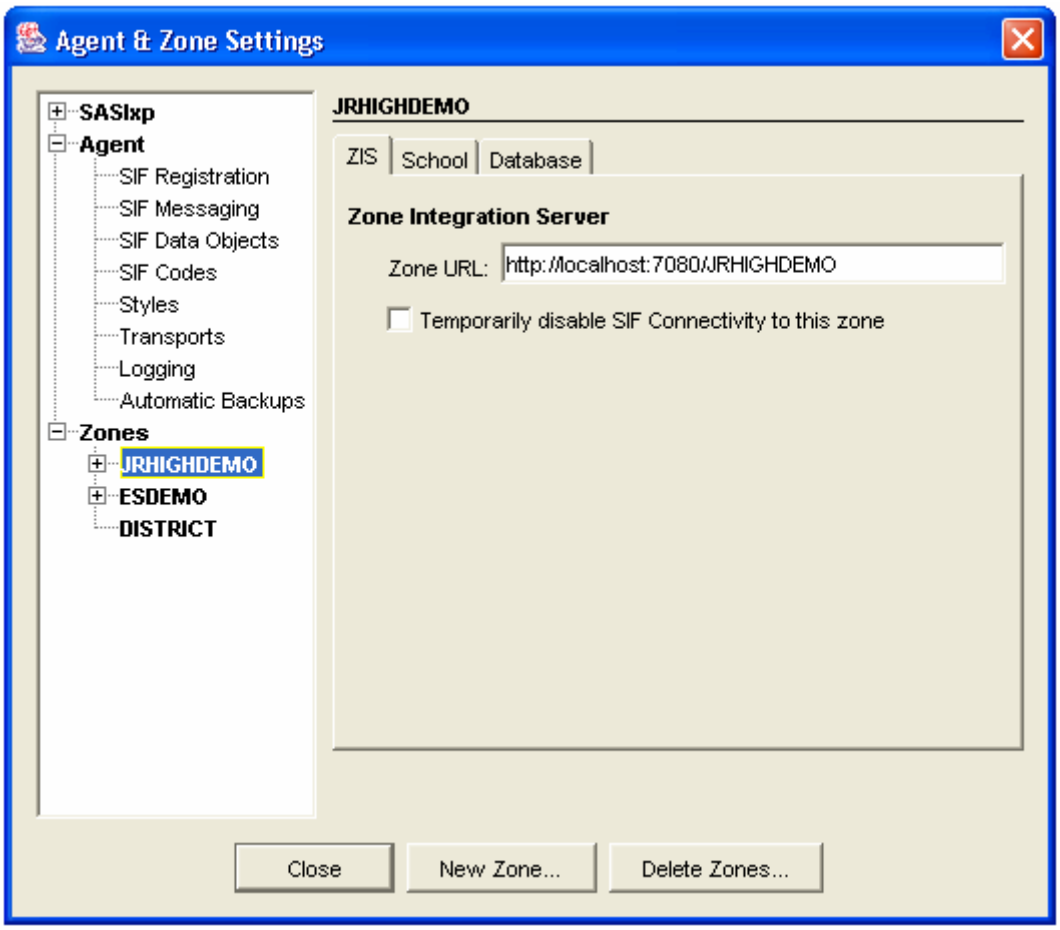


10. Click the Test button to test that the zone properties are correct. If the agent is able to successfully connect to the Zone Integration Server, a message box will be displayed indicating so. If an error occurs during the test, a message box is displayed with detailed error information.

11. Click OK to save your changes. The new zone is added to the Zones tree in the Agent & Zone Settings dialog box and is also added to the main window of the Console.

Changing Zone Properties

Once a zone is created, it's displayed in the Zones tree on the Agent & Zones Settings dialog box. You can change zone properties at any time by highlighting the zone in the tree.



Temporarily Disabling a Zone

On occasion it may become necessary to disable all connectivity between a SASIxp zone and the zone integration server. For example, you may want to temporarily stop publishing data from a school but wish to leave the agent running so that other schools in the district continue to participate in SIF.

To disable SIF connectivity to a zone,

1. Select the zone in the Agent & Zone Settings dialog box tree

2. Click the "Temporarily disable SIF Connectivity to this zone" checkbox

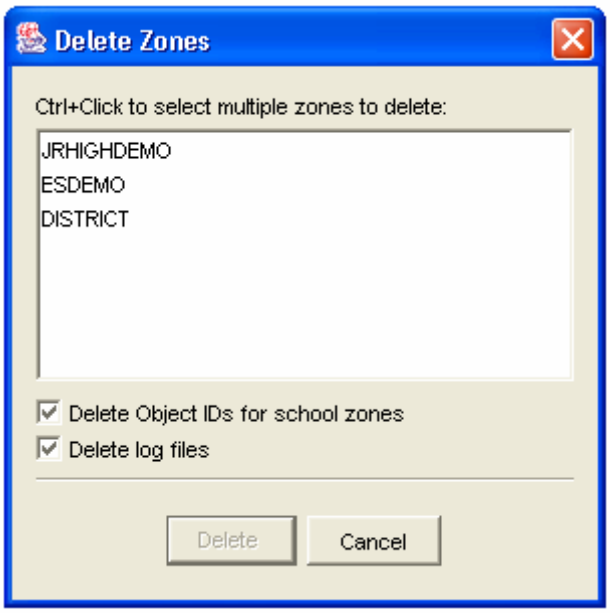
3. Close the Agent & Zone Settings dialog box. The zone's status on the main window will be shown as "Disabled" instead of "Idle".

NOTE: If this checkbox is selected and grayed out, it means a New Year Rollover is in progress. The New Year Rollover Wizard disables all zones. To ensure that an administrator does not re-enable a zone while a New Year Rollover is in progress, it also disables the checkbox.

Deleting Zones

Follow these steps to delete zones from the SASIxp agent:

1. Start the agent if not already running
2. Click on the SIF logo on the system tray to open the Console
3. Choose **Settings** from the Tools menu
4. Click the **Delete Zones…** button
5. The Delete Zones dialog box will appear



6. Select the zones to delete. You can select more than one zone by holding down the Ctrl key while clicking a zone in the list.
7. Click the Delete button to delete the selected zones

Deleting Object IDs

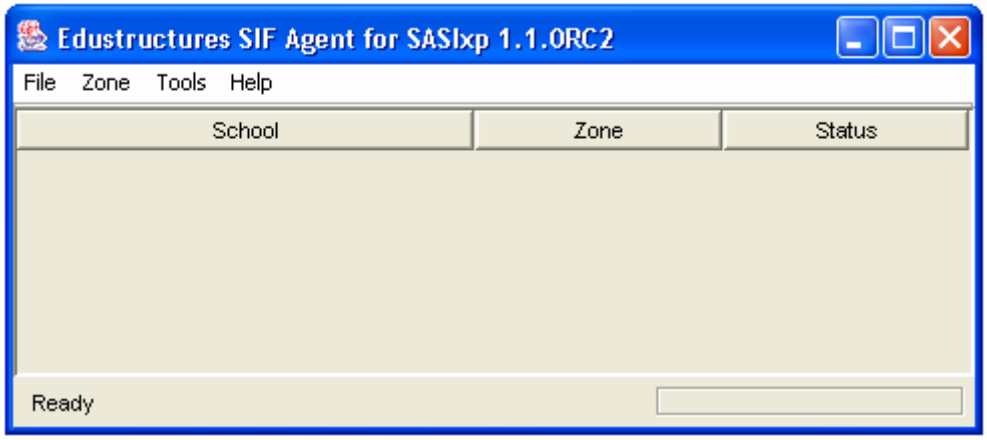
Check the "Delete Object IDs for school zones" checkbox to permanently delete all SIF object identifiers—or *RefIds*—associated with the school. While this does not impact records in the SASIxp database whatsoever, it does permanently remove the association between SASIxp records and their corresponding SIF Data Objects. Consequently, any SIF Agents that have already synchronized with the deleted zones will now reference objects that no longer exist.

Part III

ADMINISTRATION & ADVANCED CONFIGURATION

The Console

The SASIxp SIF Agent console is where configuration and administration tasks are performed. To open the console, click the blue and yellow SASIxp agent icon on the taskbar.



The Console's main window shows a list of zones to which the agent connects.

Zone Status

Although the SASIxp agent is designed to run unattended, the Console can provide a good picture of the activity taking place on each zone and whether any errors have occurred that require attention. The main window summarizes zone status with an icon and a message in the Status column for each zone.

One of three status icons may be displayed beside a zone:

Icon	Status	Description
	OK	The zone is connected to both the SASIxp database and the zone integration server and is idle or performing activity, and Event Reporting is functioning properly if enabled. No attention is required.
	Warning	A warning condition has arisen that may or may not require

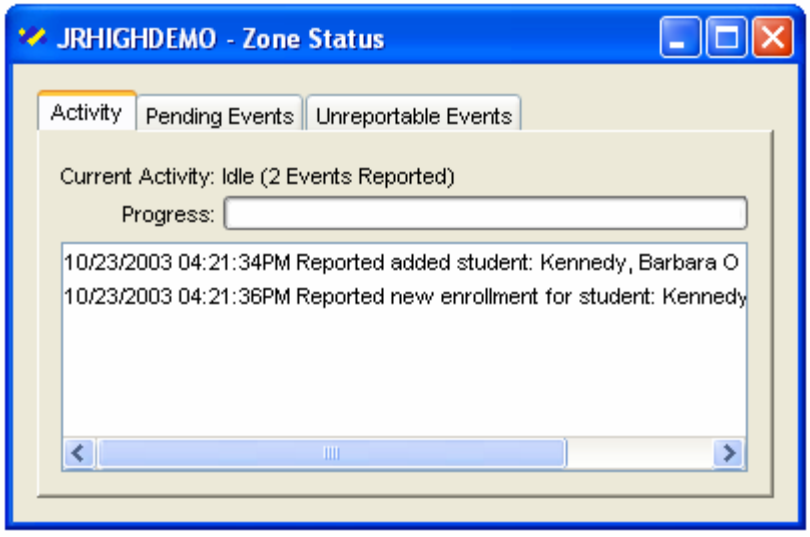
attention:

1. Event Reporting has been suspended because of a database or network connection error. The agent will automatically retry the operation in 5 minutes. If the warning status persists, open the Zone Status dialog box as described below to investigate.
2. The zone is disabled—that is, an administrator checked the "Temporarily disable SIF Connectivity to this zone" option in the Settings dialog box, or the New Year Rollover Wizard has disabled all zones during a rollover operation

Error — An error condition has arisen that requires attention:

1. The SASIxp database is not available
2. The Object IDs Database is not available
3. The connection to the zone integration server is not available
4. Event Reporting has encountered a fatal error. Details are available from the Activity tab of the Zone Status dialog box. An administrator must manually re-start Event Reporting from this dialog box.

To view more detailed status information, open the Zone Status window by double-clicking a zone in the main window or choosing "Zone Status…" from the Zones menu.



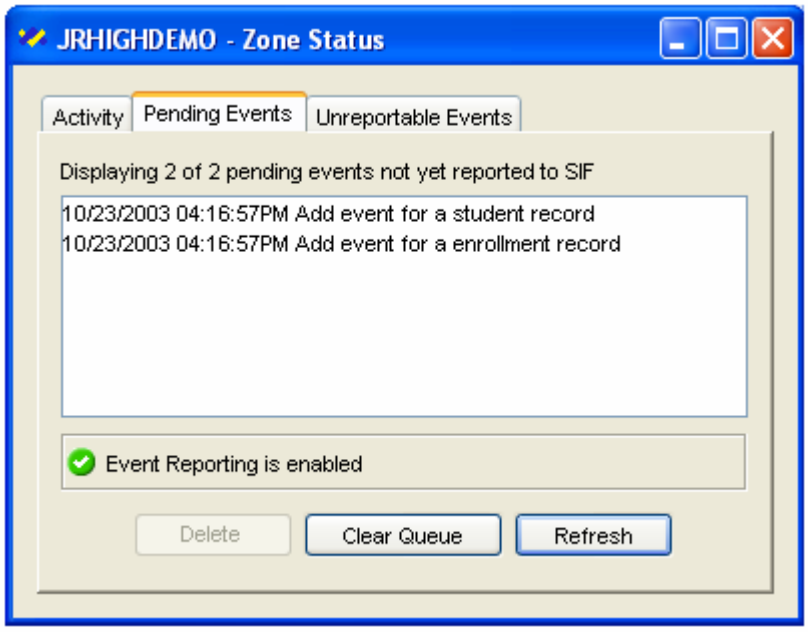
Activity Tab

The Activity tab lists the most recent 100 operations that have been performed on this zone. Whenever the agent responds to a SIF Request for data or reports a SIF Event, a new entry is displayed in the list. If the agent is performing an operation that may take some time to complete, the progress gauge will illuminate.

Note a permanent copy of the activity log is stored in the activity.log file in the agent's "\logs*zone*" directory. You can view this file in a text editor such as Notepad.

Pending Events Tab

The Pending Events tab lists the records from the SASIxp AEVT event transaction log that have not yet been reported as SIF Events. Because it may take some time to read from the SASIxp database when the agent is connected to a large number of zones on a slow network, the list does not automatically refresh. Click the Refresh button to update the display.



To clear all pending events, click the Clear Queue button. To delete a specific event, select it in the list and click the Delete button.

Deleting pending events is not generally recommended because the change information will not be reported to subscribing SIF Agents. Nonetheless, there are two cases when it is useful:

1. When Event Reporting has been disabled for an extended period of time (i.e. weeks or months), and you have since re-synchronized subscribing agents in the zone, it is recommended that the Clear Queue button be used to purged the AEVT file of all pending changes. Otherwise, the agent will report SIF Events that may reflect changes prior to the re-synchronization. This has the

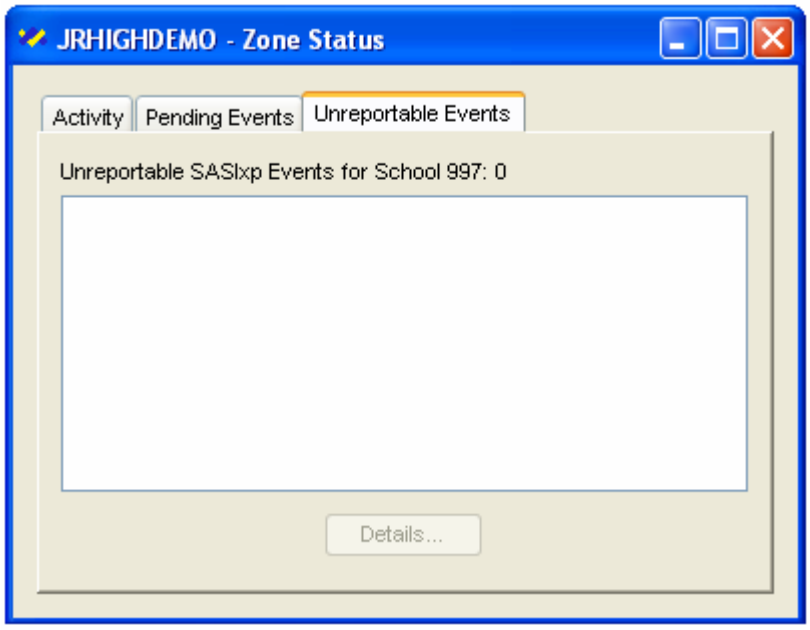
potential to introduce stale data into subscribing SIF Agents.
This is a rare occurrence; most districts keep Event Reporting enabled throughout the school year.

2. In some situations you may find that the agent is unable to report a particular event because of a problem with the software or the SASIxp database. To "unblock" the queue, select the offending entry from the Pending Events list and click the Delete button.

In addition, the Event Reporting status is shown at the bottom of the Pending Events tab. If Event Reporting has been "suspended" or stopped because errors are preventing it from working properly, the icon and status message will reflect this state. A **Details…** button will appear from which you can view the error that caused Event Reporting to suspend or stop.

Unreportable Events Tab

The Unreportable Events tab lists any data changes that could not be reported because of an error—usually a defect in the software or a customization to SASIxp that was not anticipated by the agent. To view the technical details associated with the event, select an entry in the list and click the Details button.

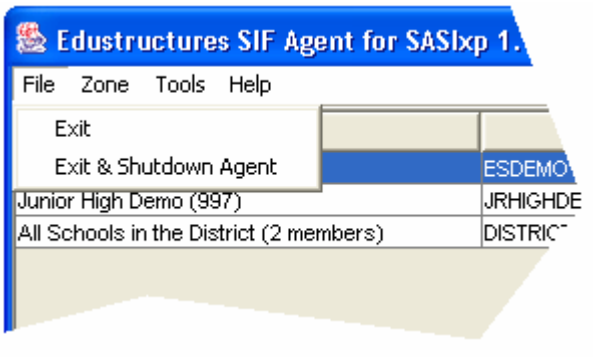


The Menu Bar

The Console's commands are organized under three menus on the menu bar:

File Menu

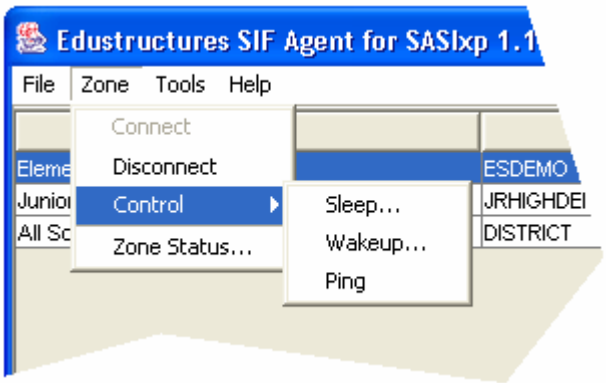
The File menu is used to exit the agent:



Menu Item	Description
File	
Exit	Exits the Console but leaves the agent running. The SIF icon does not disappear from the Windows taskbar. This command has the same affect as closing the Console window with the X in the upper, right-hand corner of the title bar.
Exit & Shutdown Agent	Exits the Console and stops the SASIxp Agent. The SIF icon will disappear from the Windows taskbar. Alternatively, the agent may be stopped from the Windows Service Manager (when running as a Service) or by pressing Ctrl+C in the Java console when running as a standalone program.

Zone Menu

The Zone menu is used to manage connections to SIF Zones or to display the Zone Status window for the highlighted zone. Note that zones cannot be added and removed from this menu; instead, use the Tools > Settings… command.

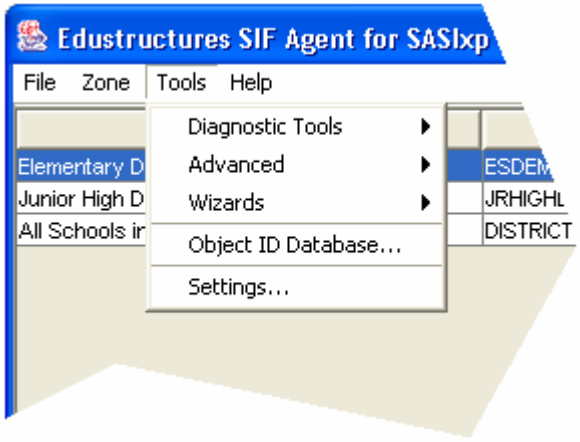


Menu Item	Description
Zone	
Connect	Establishes a connection to the zone that's highlighted in the main window. This command is grayed out if the highlighted zone is currently connected.

Disconnect	Disconnects the agent from the zone integration server that manages the zone that's highlighted in the main window.
Control > Sleep	Informs the zone integration server that the agent does not wish to accept any messages. This command is grayed out if the agent is currently sleeping. Note: The agent normally places each zone in Sleep mode when the NT Service is stopped.
Control > Wakeup	Wakes up a zone that has previously been put into Sleep mode. Note: The agent normally wakes up each zone when the NT Service is started.
Control > Ping	Sends a "SIF Ping" request to the zone integration server for the highlighted zone to verify that the agent and server are connected and communicating.
Zone Status	Opens the Zone Status window from which you can view activity and status information regarding the highlighted zone. NOTE: You can also double-click a zone in the main window to open the Zone Status window for that zone.

Tools Menu

The Tools menu is used to access the Agent & Zone Settings dialog box and the Object ID Database status window, as well as to perform specialized administrative tasks such as manually generating SIF Events for SASIxp records.



Menu Item	Description
Tools > Diagnostic Tools	
SASIxp Database Performance	Opens the SASIxp Database Performance dialog box to test how quickly the agent accesses the SASIxp database for each zone.
SASIxp Event Monitoring	Opens the SASIxp Event Monitoring dialog box to check the event monitoring configuration of SASIxp at each school. This tool should be run at initial installation

	time. It prepares a report of the SASIxp database files and fields that are monitored for changes, and also offers an option to repair the configuration if it is incompatible with the requirements of the agent.
Tools > Advanced	
Prepare Enrollment Data	Opens the Prepare Enrollment Data dialog box to optionally prep student enrollment records for SIF. This tool should be used at initial installation time. The preparation of enrollment data is normally handled automatically the first time an agent requests enrollment records from a school. However, this process can be very time consuming if the agent is accessing SASIxp data files over a slow network connection. It is much faster when performed ahead of time using this tool.
Tools > Wizards	
HTTPS Wizard	The HTTPS Wizard assists administrators in creating digital certificates and configuring the agent's transport protocols for secure HTTPS communication with the zone integration server.
New Year Rollover Wizard	The New Year Rollover Wizard must be used both before and after the SASIxp New Year Rollover procedure. It reconciles student identifiers in the new school year with identifiers stored in the Object ID Database, reports SIF Events by comparing new school year data to the previous year's, and cleans out the AEVT Event Transaction Log so that changes made to the database during the NYR procedure are not propagated to the SIF infrastructure.
Tools	
Object ID Database...	Opens the Object ID Database status window. Here you can view the status information regarding the database where all SIF identifiers are stored for SASIxp records. Some commands, such as backing up and restoring the database, can also be performed from the status window.
Settings...	Opens the Agent & Zone Settings dialog box

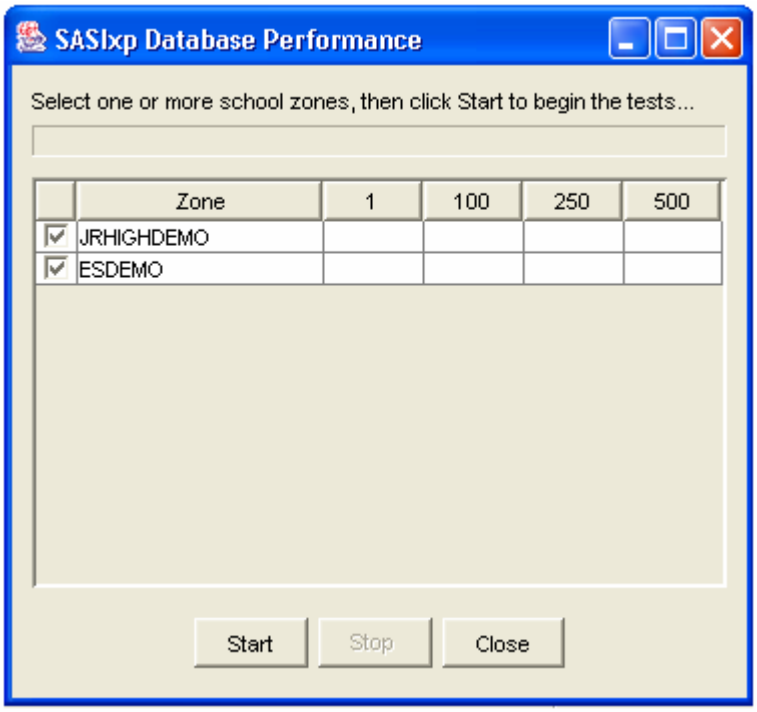
Tools

The SASIxp Database Performance Tool

The **SASIxp Database Performance** tool, found on the Console's **Tools > Diagnostic Tools** menu, prepares a report showing the amount of time taken by the agent to read student records from each SASIxp school. This information can be helpful in determining the relative speed at which the agent accesses SASIxp databases over the network compared to accessing database on the local computer. It is also used to note the speed of the agent at different times of the day and in diagnosing performance-related issues after installation.

To prepare a SASIxp Database Performance report,

1. Start the agent if not already running
2. Click on the SIF logo on the system tray to open the Console
3. Choose **SASIxp Database Performance** from the Tools > Diagnostic Tools menu



4. Optionally exclude one or more zones from the test by clearing the checkboxes
5. Click the Start button to run the report

When the report is complete, the results are written to a log file in the agent's "logs" directory.

Interpreting the Results

This tool works by first reading *all* student records from the SASIxp database. The time taken by this operation is displayed in the first column, labeled "1". Next, the tool enumerates the first 100 students in the list, querying the database for each student individually, and displays the time taken in the second column labeled "100". The time to perform this test will be significantly greater than the first test because the agent must issue 100 individual queries to the database instead of just one query. This test is again performed for the first 250 and 500 students in the list, respectively, with the results displayed in the "250" and "500" columns.

If the SASIxp database is located on the same computer as the agent (i.e. the agent does not need to access data files over the network), the results will be similar to what's shown below for a school with 800 or so student records.

1	100	250	500
2 seconds	5 seconds	13 seconds	30 seconds

800 students – dBASE IV access on local computer

When the agent is connected to this same school over a 100MB LAN network connection, the SASIxp Database Performance tool shows that database access times are increased but still acceptable (3 seconds to request all students from the school versus 2 seconds):

1	100	250	500
3 seconds	30 seconds	84 seconds	179 seconds

800 students – dBASE IV access over the LAN

When the agent is accessing dBASE IV files over a very slow network connection—in this case a 256K VPN link—the results differ considerably. In this case it took 92 seconds to read all students from the school versus the 2 or 3 seconds above. Given these results, the administrator might decide to install the agent on the same computer where SASIxp's data files are located to avoid the slow network connection:

1	100	250	500
92 seconds	seconds	seconds	seconds

800 students – dBASE IV access over a very slow 256K network connection

The SASIxp Event Monitoring Tool

The **SASIxp Event Monitoring** tool, found on the Console's **Tools > Diagnostic Tools** menu, prepares a report showing the database files and fields that SASIxp is configured to monitor for the purpose of reporting SIF Events. It's also capable of repairing the event monitoring configuration if it does not contain the entries needed by the agent for proper operation.

The SASIxp Event Monitoring tool should be used after initial installation to verify that event reporting is configured properly. Edustructures Technical Support may also have you run this tool to help diagnose problems with SIF Event reporting.

Background

When the database "monitoring" feature of SASIxp is enabled, SASIxp keeps track of all changes made to its database so that they can be reported as SIF Events by the agent. When a change is made to a monitored field—for example, a new student is added or a student's telephone number is edited—the change is recorded in the AEVT Event Transaction Log file. The agent periodically checks this log for new entries; if any are found, they're reported as SIF Events and removed from the file. This is the basic underlying mechanism that makes it possible for SASIxp to support SIF event reporting.

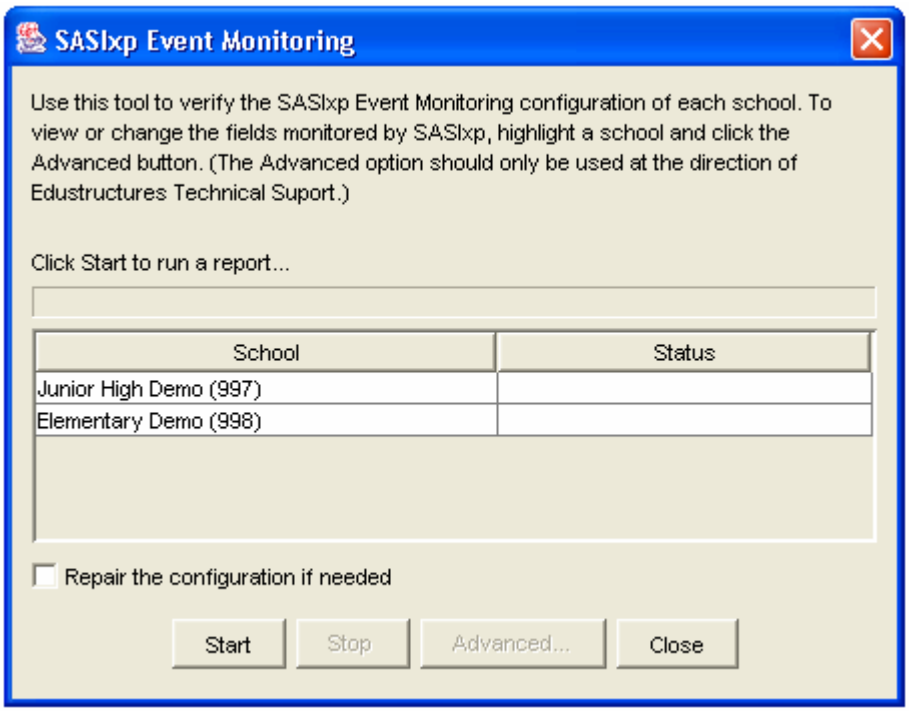
For performance reasons, SASIxp does not monitor *all* database files and fields because only a small subset of these are actually used by SIF. Instead, it monitors only the specific files and fields listed in the configuration files AFLM and AFDM. Thus, the way the agent tracks changes to SASIxp records is determined by the configuration of SASIxp and not the configuration of the agent. If the AFLM and AFDM files do not contain the expected set of entries, the agent won't function properly.

Some versions of SASIxp—especially patches to the software—include varying AFLM and AFDM files that do not always contain the required set of files and fields expected by the SIF Agent for proper operation. To ensure these files are compatible with the agent, it's recommended that administrators replace them with the AFLM and AFDM files included in the agent's "extras" directory. Alternatively, you can use the **SASIxp Event Monitoring** tool to analyze and repair these files if needed.

Using the Tool

Follow these steps to use the tool:

1. Start the agent if not already running
2. Click on the SIF logo on the system tray to open the Console
3. Choose **SASIxp Event Monitoring** from the Tools > Diagnostic Tools menu



4. Click the Start button to run the report

When the report is complete, the results are written to a log file in the agent's "logs" directory. The "Status" column will indicate if repairs need to be made to the configuration. If so, click the "Repair the configuration if needed" checkbox and click the Start button again. This time the tool will add the necessary entries to the AFLM and AFDM files at each school so that event monitoring will function properly.

▸ **IMPORTANT:** If the tool indicates that it has made changes to the AFLM and AFDM files when the Repair checkbox is marked, you must run a Reorg on these two files from SASIxp's File Management folder and then restart the SASIxp application for the changes to take effect.

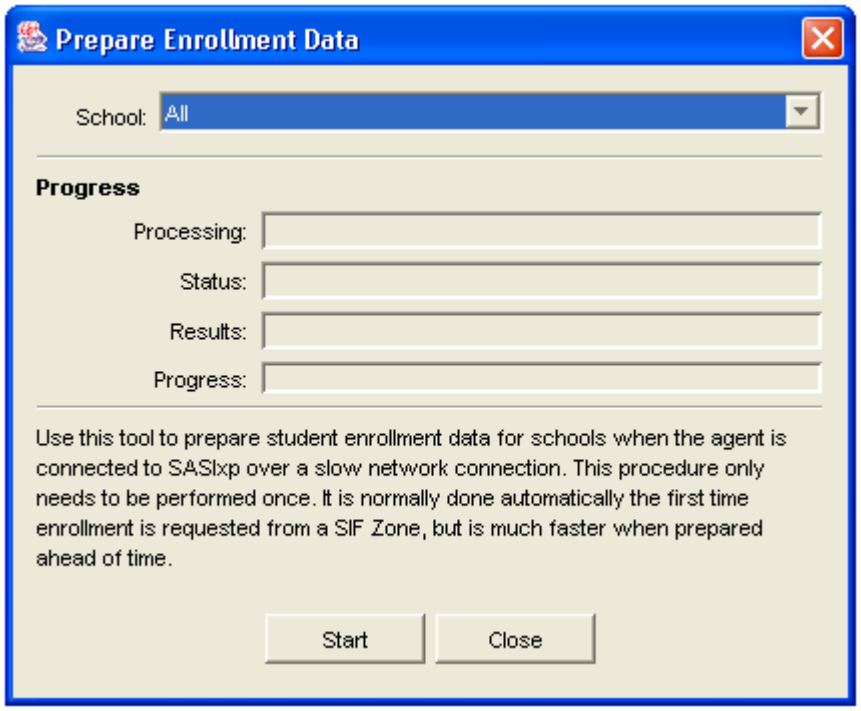
The Prepare Enrollment Data Tool

The **Prepare Enrollment Data** tool, found on the Console's **Tools > Advanced** menu, populates the agent's Object ID Database with SIF RefIds for all student enrollment records. This processing is normally handled by the agent the first time enrollment data is requested from a zone, but can take a very long time to complete over a slow network connection. To avoid this initial performance hit, you can use the Prepare Enrollment Data tool to force the agent to populate its Object ID Database ahead of time.

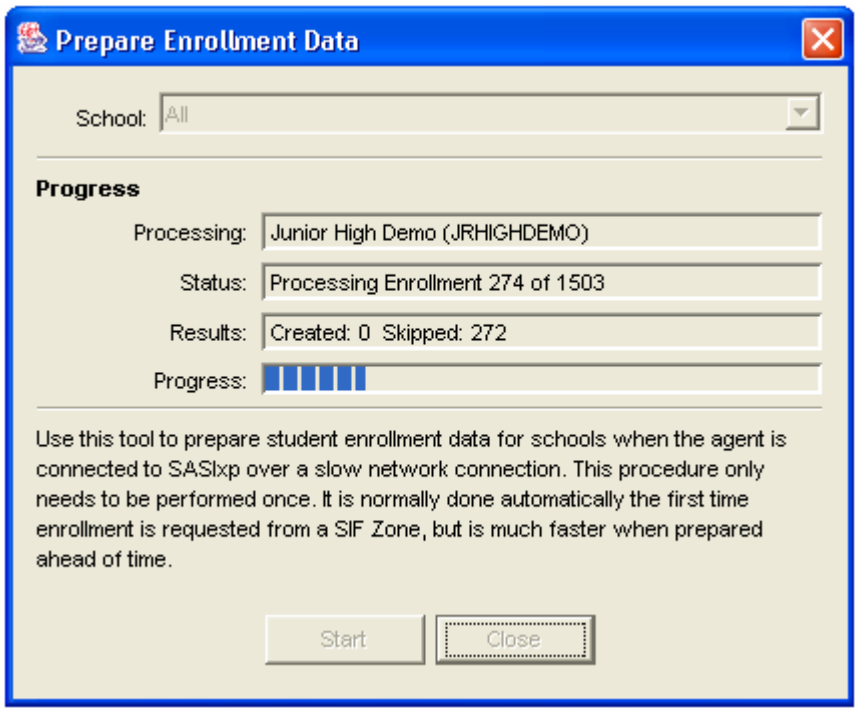
▸ **NOTE:** This optional procedure is automatically performed when a new zone is created. The Prepare Enrollment Data tool is available so that administrators can manually perform this task in the event the New Zone dialog box encounters a database or connection error.

Follow these steps to use the tool:

1. Start the agent if not already running
2. Click on the SIF logo on the system tray to open the Console
3. Choose **Prepare Enrollment Data** from the Tools > Advanced menu



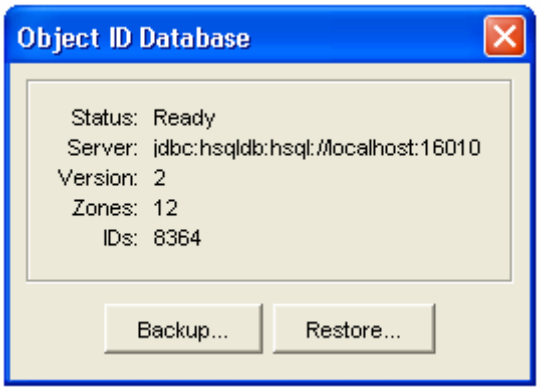
4. To prepare enrollment data for a specific school, choose it from the "School" combo-box. Otherwise, choose "All" to run the tool on all school zones.
5. Click the Start button



Object ID Database

The Object ID Database is an integral part of the agent that must be running at all times. This database is used to store the unique identifiers, or "RefIds", of each SIF Data Object, and also includes information to associate each RefId with its corresponding record in the SASIxp database.

To view the status of the Object ID Database, choose **Object ID Database** from the Tools menu. The following dialog box appears:



If the database is on-line and the agent is connected to it, the **Status** field shows a value of "Ready".

The **Server** field displays the database driver, server address, and port of the database. If the Object ID Database is running on a different computer than the SASIxp agent, you can verify that the agent is configured with the correct address and port number here. (See the Advanced Configuration section for more information about changing the location of the Object ID Database.)

The **Version** field is the version of the database schema in use—currently version 2. Earlier releases of the SASIxp agent used version 1. If an upgrade to the database schema is available, an "Upgrade…" button will be shown at the bottom of the dialog box. Clicking this button upgrades the database in place.

The **Zones** and **IDs** fields indicate the number of zones represented in the database and the total number of RefIds recorded.

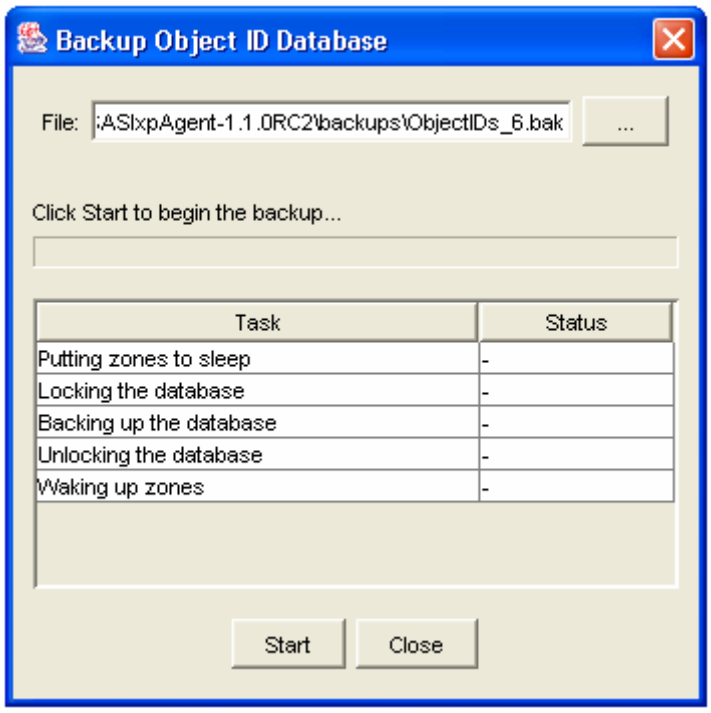
Backing up the Object ID Database

RefIds are important because they track the relationship between SASIxp records and SIF objects. If the Object ID Database is damaged or lost for any reason, all SIF Agents that have requested SIF objects from SASIxp will need to be resynchronized because the identifiers for these objects would no longer exist and new ones would be generated by the agent. Consequently, you should make a regular backup of the Object ID Database so that it can be restored if damaged or lost.

When Automatic Backup is enabled (the default), the agent backs up the database daily at a set time. Refer to the *Automatic Backup Settings* on page 49 for more information on the Automatic Backup feature.

To manually backup the Object ID Database,

1. Start the agent if not already running
2. Click on the SIF logo on the system tray to open the Console
3. Choose **Object ID Database** from the Tools menu
4. Click the Backup… button. The Backup Object ID Database dialog box appears:



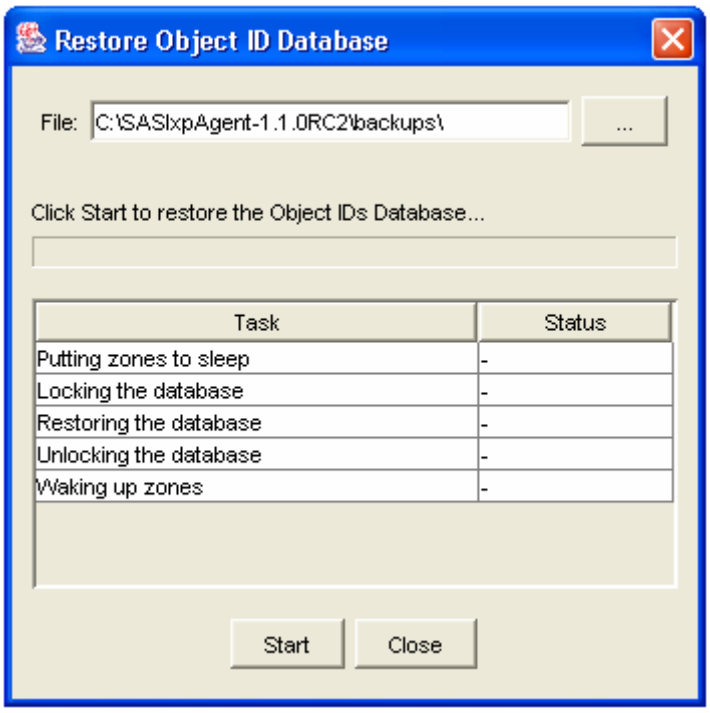
Type the name of the backup file in the **File:** field, then click the Start button. All entries in the database are written to the backup file you specify. Note that backup files are simply text files written in a special format that the agent can understand; you can view them in Notepad or another text editor.

Note that prior to performing a backup, all zones are put to sleep to prevent SIF activity from interfering with the backup process. When complete, all zones are woken up.

Restoring the Object ID Database from a Backup

To restore the database from a backup file,

1. Start the agent if not already running
2. Click on the SIF logo on the system tray to open the Console
3. Choose **Object ID Database** from the Tools menu
4. Click the Restore… button. The Restore Object ID Database dialog box appears:



Browse to the backup file or type the name of the file into the **File:** field, then click the Start button to restore the database.

▸ **IMPORTANT:** Restoring the Object ID Database from a backup file completely replaces all records in the database with the RefIds in the file. In other words, the database is first cleared of all records before the restoration is performed.

Part IV

ADVANCED CONFIGURATION

Security

The SASIxp agent communicates with zone integration servers using the HTTP or secure HTTPS transport protocols. HTTPS is a secure version of HTTP commonly used by e-commerce websites. It provides for both encrypted and authenticated communications so that data sent over the network is not only protected from view but also verified to be exchanged between two parties that trust one another. HTTP works the same as HTTPS but does not offer any encryption or authentication capability.

Authentication

HTTPS may be used in two modes:

- Server Authentication
- Client & Server Authentication

When Server Authentication is used, the zone integration server presents its security credentials to the SASIxp agent for verification each time the agent sends a message to the server. If the agent does not trust that the server is who it claims to be, the connection is not established. With Server Authentication, the agent knows that it is transmitting SIF information to the zone integration server instead of to a third-party claiming to be the zone integration server.

When Client Authentication is used, both sides of the communication present their security credentials for verification. Client Authentication ensures that the zone integration server sends SIF messages to the SASIxp agent at a specified server address, so that another party cannot act as an imposter by registering its own SASIxp agent with the server.

With both Server Authentication and Client Authentication, the entity asking for a certificate must *trust* that certificate for the communication to proceed. This trust is established when both parties have one another's digital certificate on file.

Preparing for HTTPS

To use HTTPS you'll need:

1. A digital certificate signed by a trusted Certificate Authority (CA). You have at least three choices for obtaining a certificate: Create your own "self-signed" certificate using the SASIxp agent's HTTPS Wizard; establish your own Certificate Authority with software available from Microsoft, Netscape, and others; or purchase a signed certificate from a third-party CA such as VeriSign.

2. The zone integration server's digital certificate. You'll import this certificate into the agent's "truststore"—a file that keeps track of the certificates the agent will trust when establishing connections to zone integration servers.

In addition, when using Client Authentication the zone integration server will need a copy of the SASIxp agent's certificate as well so that it can trust the agent. Consult your ZIS documentation for instructions on setting up HTTPS at the zone integration server.

Creating and Importing Certificates for HTTPS

The first step in configuring the agent to use HTTPS is to create a *private key* and a *keystore* that contains that private key. A keystore is a file that holds keys and certificates. When the agent is installed, its keystore files—`Agent.ks` and `Trusted.ks`—are empty. The `Agent.ks` file stores the private key and public certificate of the SASIxp agent, while the `Trusted.ks` file stores the certificates of zone integration servers that are trusted by the agent.

Method 1: Creating a Self-Signed Certificate

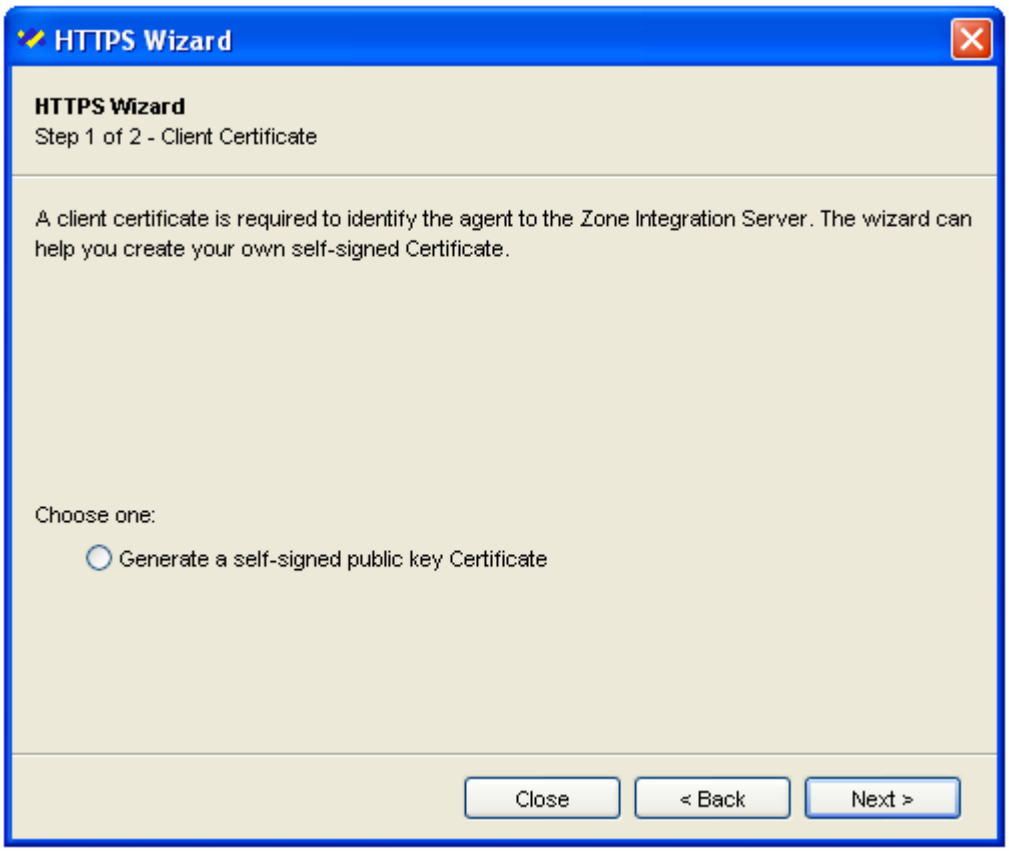
The easiest and least expensive way to create and prepare signed public key certificates is to simply create your own. These so-called "self-signed" certificates are not signed by any third-party Certificate Authority and are trusted only by you.

Follow these steps to create a new self-signed certificate for the SASIxp agent:

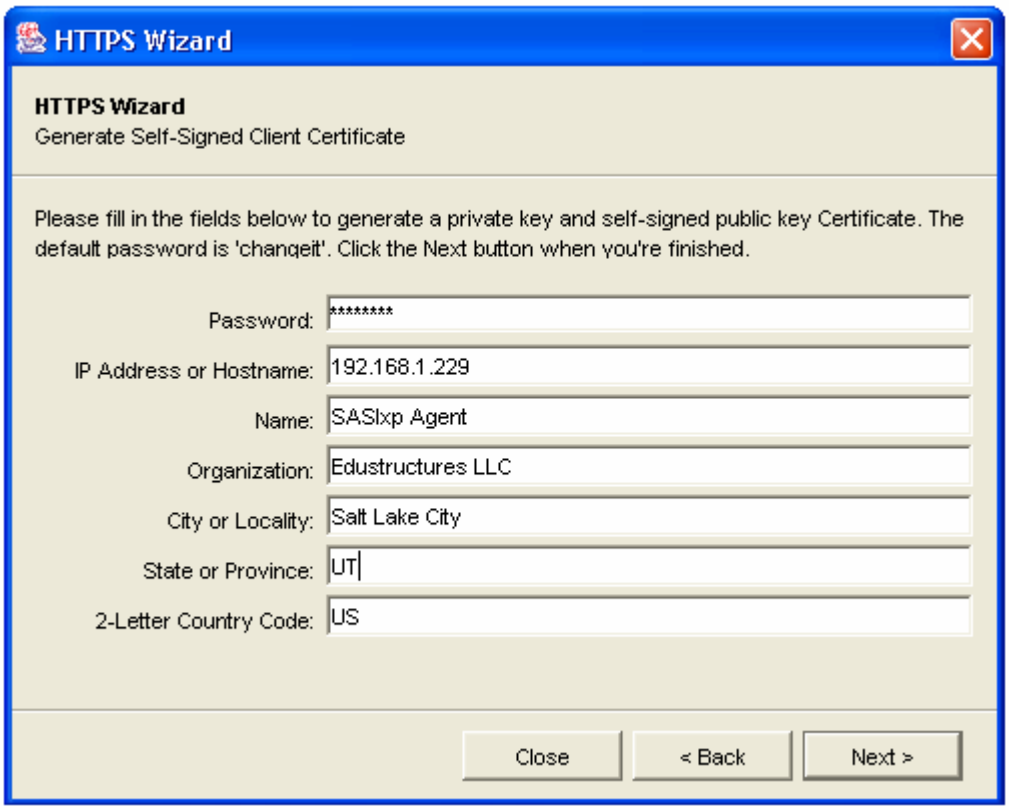
1. Start the agent if not already running

2. Click on the SIF logo on the system tray to open the Console

3. Choose **HTTPS Wizard** from the **Tools > Wizards** menu



4. On the second page of the wizard, choose the first radio button: "Generate a self-signed public key certificate", then click the Next button.



5. Fill in the fields.

   Password: If this is the first time you've run the wizard and the agent's keystore files do not yet exist, enter the password you want to assign to those files. The default is "changeit". If you've previously used the wizard and the agent's keystore files have already been created, enter the password that you used to initially create the files. Again, the default is "changeit".

   IP Address or Hostname: Enter the IP address where the agent is running

   Name, Organization, City, etc. These fields are optional but recommended.

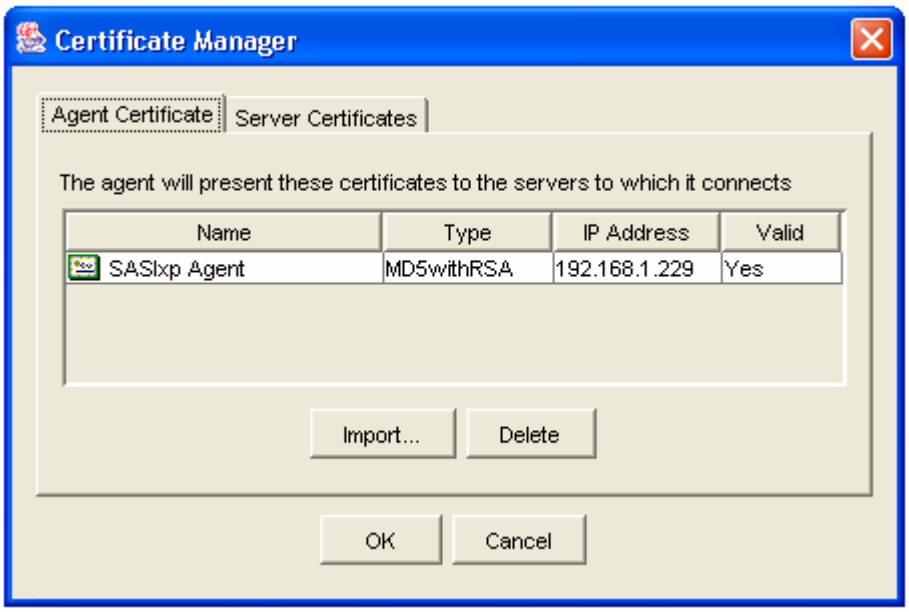
6. Click next to generate a certificate and import it into the agent's keystore.

When the wizard has completed, click the Finish button to close it. Next, follow the steps below to verify that the wizard created a certificate and imported it into the agent's keystore:

7. Choose **Settings** from the Tools menu

8. Click on the Transports node in the tree, then select the HTTPS tab

9. Click the Certificate Manager button



This dialog box shows the Agent Certificate in the `Agent.ks` file, which is modified by the HTTPS Wizard and should now consist of one entry having the IP address or hostname you entered in step 5 above. The Server Certificates tab lists the trusted zone integration server certificates that are stored in the agent's `Trusted.ks` file. You can use the Import and Delete buttons on this dialog box to manually import digital certificates instead of using the HTTPS Wizard.

Trusting the Zone Integration Server's Certificate

Now that you've created a self-signed certificate, the second step in setting up HTTPS is to obtain the zone integration server's certificate so that the agent will trust it when establishing a connection to each zone. This can be done with the by clicking the Import button on the Server Certificates page of the Certificate Manager (shown in the previous section); or, you can use the HTTPS Wizard to import the server certificate.

Follow these steps:

1. Using the tools provided by your zone integration server product, export its digital certificate to a file. This file will be imported into the SASIxp agent so that the server is trusted when establishing a connection.

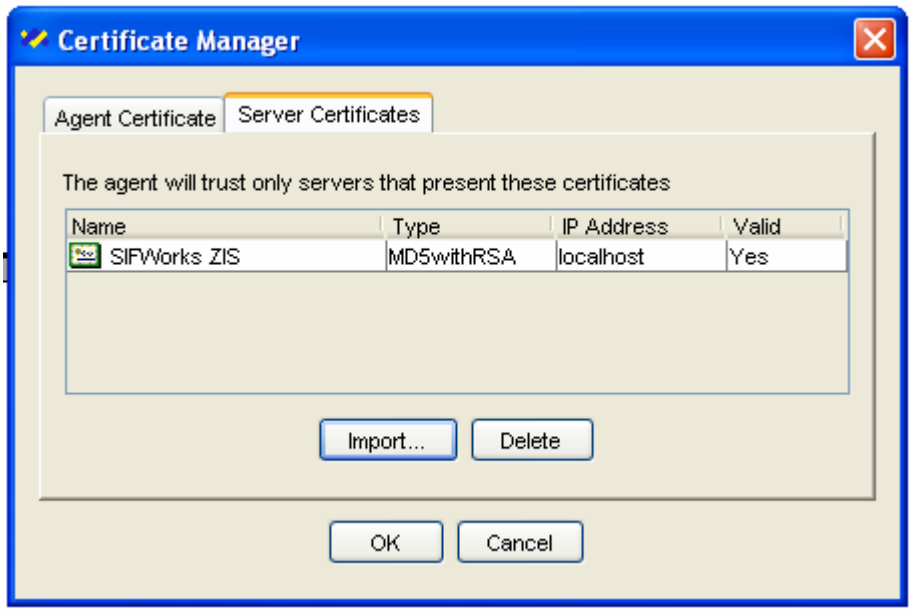
2. Start the agent if not already running

3. Click on the SIF logo on the system tray to open the Console

4. Choose **Settings** from the Tools menu

5. Click on the Transports node in the tree, then select the HTTPS tab

6. Click the Certificate Manager button



Click the Server Certificates tab to display the zone integration server certificates trusted by the SASIxp agent. To import your ZIS certificate, click the Import… button and browse to the certificate file that was exported in Step 1. Click OK to save your changes. The SASIxp agent is now configured to trust the certificate of your zone integration server.

Configuring the Agent & Zones for HTTPS

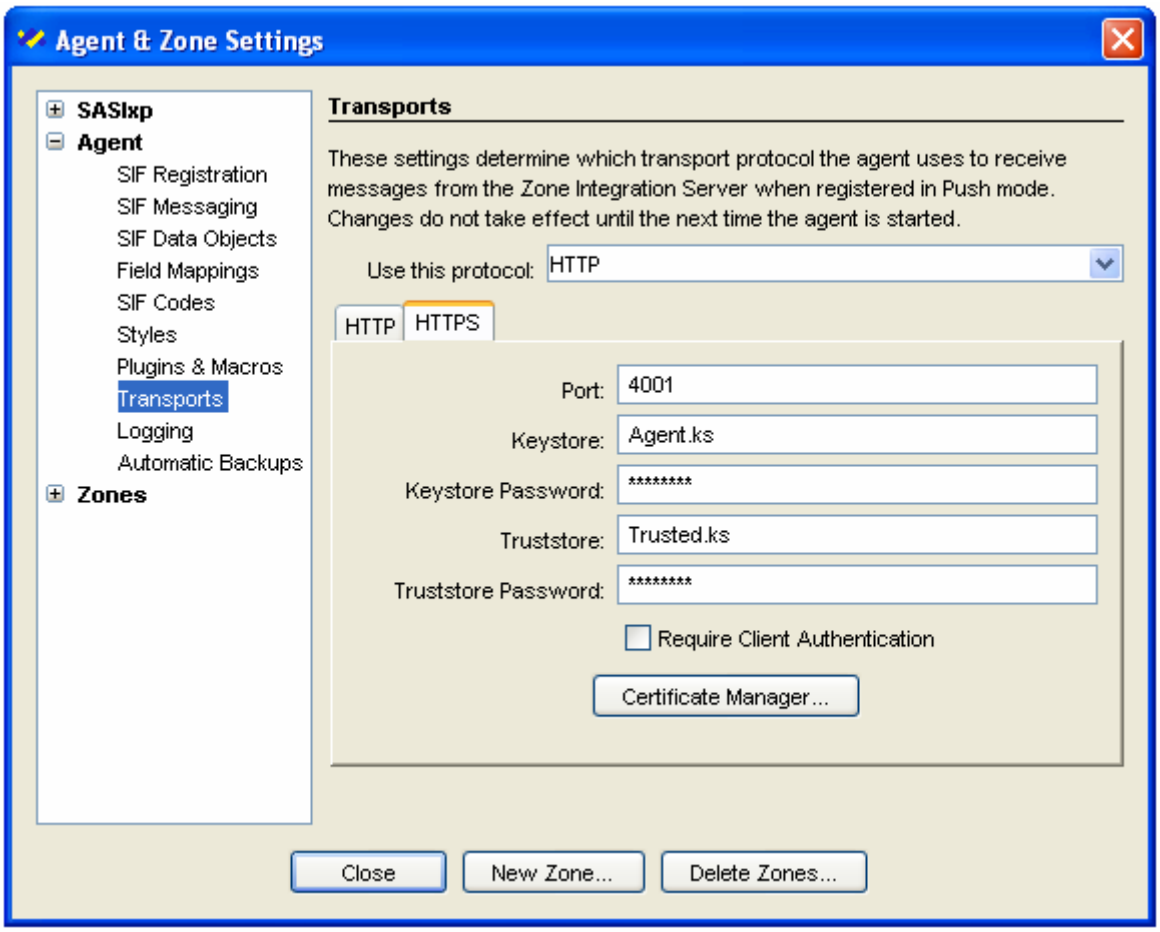
Once certificates have been configured as described in the preceding section, the final step to enabling HTTPS is to change the agent's transport protocol and zone settings.

Transport Protocol Settings

When the agent runs in Push mode, it establishes an HTTPS port to listen for incoming traffic sent by the zone integration server. The transport protocol and port settings are configured in the Agent & Zone Settings dialog box.

Follow these steps to set the transport protocol to HTTPS

1. Start the agent if not already running
2. Click on the SIF logo on the system tray to open the Console
3. Choose **Settings** from the Tools menu
4. Click the Transports node in the tree



5. Select HTTPS from the "Use this protocol" combo-box

6. Click the HTTPS tab and verify that the field values are correct. Here you can specify a port number to listen for incoming traffic, change the agent's keystore and truststore files, and enable Client Authentication. By default, the SASIxp agent uses port 4001 for HTTPS connectivity. If another application is using this port you can change it to another value.

7. Close the Settings dialog box and restart the agent for the changes to take effect

Zone URL Settings

The zone integration server URL of each zone must match the protocol used by the agent. For example, if the agent's transport protocol is set to HTTPS as described in the preceding section, then the URL of each zone must be changed to "https://". Follow these steps for each zone the agent is connected to:

1. Start the agent if not already running

2. Click on the SIF logo on the system tray to open the Console

3. Choose **Settings** from the Tools menu

4. Select a zone in the tree

5. On the Zone Integration Server tab, verify that the URL begins with "https://" if the agent is configured to use the HTTPS transport protocol.

6. When the Settings dialog box is closed the agent will reconnect to each zone using the new URL

▸ **NOTE:** In this version of the SASIxp agent, all zones must use the same transport protocol, and it must match the protocol selected in the Settings dialog box. You cannot, for example, configure some zones to use HTTP and others to use HTTPS.

Part V

MAINTENANCE PROCEDURES

New Year Rollover

Like SASIxp, the agent requires that a New Year Rollover procedure be performed when transitioning from one school year to the next. This procedure is automated by the New Year Rollover Wizard, found on the Tools > Wizards menu of the agent's Console. It must be run at the end of the current school year **before** performing the SASIxp New Year Rollover procedure, and again at the beginning of the new school year **after** that procedure has been completed.

SIF End-of-Year Procedure

The Schools Interoperability Framework 1.1 standard does not prescribe an end-of-year procedure for K-12 applications to follow. However, the consensus among vendors is that the SIF infrastructure be "turned off" during the summer months while an end-of-year procedure is performed on the student information system database. This is most easily achieved by disabling the zone integration server, and will prevent SIF from propagating data while New Year Rollover procedures are being performed by district staff. Once these procedures have been completed, the zone integration server can be turned on again so that SIF interoperability will resume.

Follow these steps at the end of a school year:

1. Run the SASIxp agent's New Year Rollover Wizard as described in this section.
2. When the Wizard completes, stop the SIFWorks® Enterprise ZIS
3. If SIFWorks is running as an NT Service, open the Windows Service Manager and change the NT Service startup mode from "Automatic" to "Manual" to prevent SIFWorks from running when the computer is restarted. If SIFWorks is running from a batch file instead of as an NT Service, temporarily disable the batch file.
4. Proceed with the SASIxp New Year Rollover procedures

Once you have completed the SASIxp New Year Rollover procedures and are ready to publish the new data to SIF-enabled applications, follow these steps:

1. Start the SIFWorks® Enterprise ZIS

2. If SIFWorks is running as an NT Service, open the Windows Service Manager and change the NT Service startup mode from "Manual" back to "Automatic" so the server will run automatically each time the computer is started. If SIFWorks was running from a batch file instead of an NT Service, re-enable the batch file.

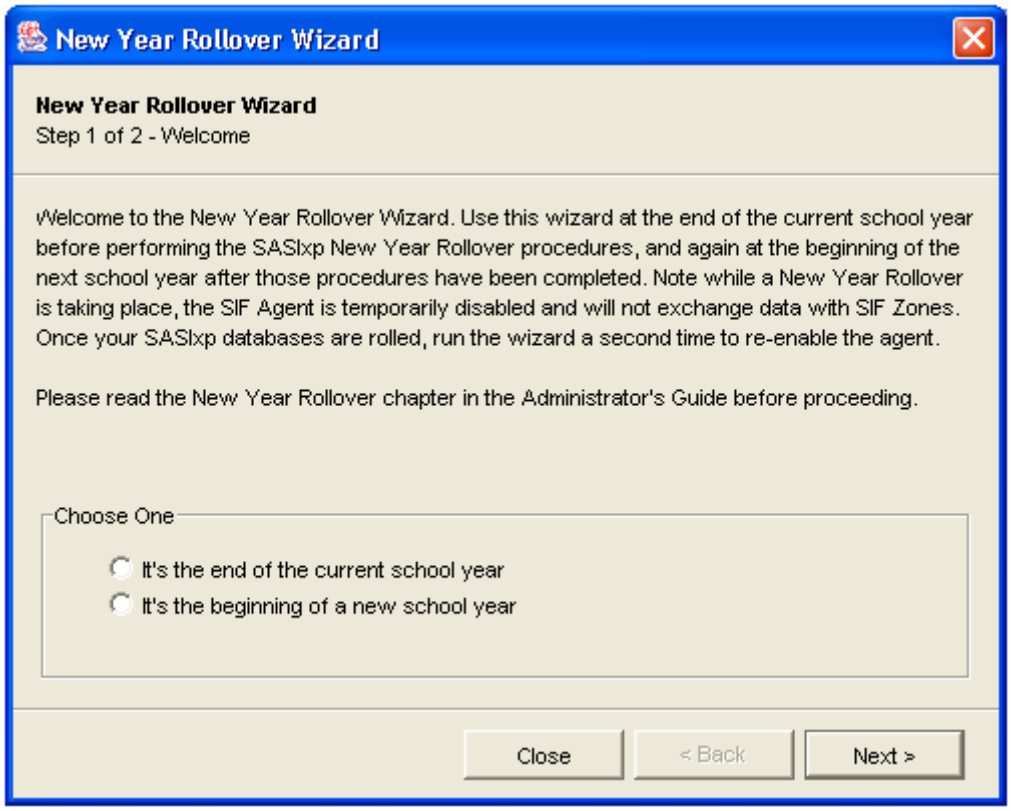
3. Run the SASIxp Agent's New Year Rollover Wizard a second time as described in this section. The Wizard will resume where it left off at the end of the school year.

4. Resynchronize any SIF Agents as necessary

New Year Rollover Wizard

The agent's New Year Rollover Wizard is designed to be used in conjunction with the SASIxp New Year Rollover procedures. You should run this wizard once **before** applying the SASIxp New Year Rollover procedure, and again **after** that procedure has been completed and you're ready to publish data from the new year to SIF-enabled applications.

When the wizard is opened, it prompts you to choose whether this is the end of the current school year or the beginning of the next school year. The actions that are taken by the wizard depend on your selection:



"It's the end of the current school year"

When this option is selected, the wizard performs these SIF maintenance tasks:

1. Disables the agent's connectivity to each SIF Zone

   This is a precautionary measure to prevent the agent from sending SIF Event messages and responding to SIF Requests while a New Year Rollover procedure is in progress

Once the wizard has completed, it is safe to proceed with the SASIxp New Year Rollover procedures.

"It's the beginning of the new school year"

When this option is selected, the wizard performs these SIF maintenance tasks:

1. Reconciles identifiers in the SIF Object IDs database with new student identifiers

   During a SASIxp New Year Rollover procedure, the internal "StuLink" identifiers of each student are changed. The agent uses these identifiers to associate SASIxp records with SIF Data Objects. During this step, the wizard reconciles student identifiers by updating the "StuLink" values in the agent's database to match those in the SASIxp database.

2. Reports SIF Events

   This optional step generates SIF Events for each supported object in the SASIxp database by comparing the Object IDs from last year with the data in each school's rolled-over database. Add events are reported if an object exists in SASIxp but was not published last year. Delete events are reported if an object exists in the Object ID database but not in this year's SASIxp database. Finally, Change events are reported for all objects regardless of whether or not any fields have actually changed. For each object type you can choose to report any combination of Add, Change, and Delete events.

3. Clears the SASIxp Event Transaction Log

   During the New Year Rollover procedure, the SASIxp Event Transaction Log file (AEVT) may be filled with records that should be deleted. The agent deletes all entries from this file before proceeding to the next step.

4. Increments the school year for each SIF Zone

   When a SIF Zone is added to the agent, the administrator specifies the school number and school year. During this step, the school year is automatically incremented.

5. Re-enables the agent's connectivity to each SIF Zone